AWS Dasar Keamanan Startup (SSB)AWS

AWS Panduan Preskriptif

AWS Panduan Preskriptif: AWS Dasar Keamanan Startup (SSB)AWS

Table of Contents

Pengantar 1
Audiens yang dituju 1
Kerangka dasar dan tanggung jawab keamanan 2
Mengamankan akun Anda 3
ACCT.01 - Tetapkan kontak tingkat akun 3
ACCT.02 — Batasi penggunaan pengguna root 4
ACCT.03 - Konfigurasikan akses konsol 5
ACCT.04 - Tetapkan izin 6
ACCT.05 — Membutuhkan MFA 7
ACCT.06 — Menegakkan kebijakan kata sandi 8
ACCT.07 - Log peristiwa 9
ACCT.08 — Mencegah akses publik ke bucket S3 pribadi 10
ACCT.09 - Hapus sumber daya yang tidak digunakan 11
ACCT.10 — Memantau biaya 12
ACCT.11 - Aktifkan GuardDuty 12
ACCT.12 — Memantau masalah berisiko tinggi 13
Mengamankan beban kerja Anda 14
WKLD.01 - Gunakan peran IAM untuk izin 14
WKLD.02 — Gunakan kebijakan berbasis sumber daya 15
WKLD.03 - Gunakan rahasia singkat atau layanan manajemen rahasia 16
WKLD.04 - Lindungi rahasia aplikasi 17
WKLD.05 — Mendeteksi dan memulihkan rahasia yang terungkap 18
WKLD.06 — Gunakan Manajer Sistem alih-alih SSH atau RDP 18
WKLD.07 - Log peristiwa data untuk bucket S3 tertentu 19
WKLD.08 - Enkripsi volume Amazon EBS 20
WKLD.09 - Enkripsi basis data Amazon RDS 21
WKLD.10 - Menyebarkan sumber daya pribadi di subnet pribadi 21
WKLD.11 — Gunakan grup keamanan untuk membatasi akses 22
WKLD.12 - Gunakan titik akhir VPC untuk mengakses layanan 23
WKLD.13 - Memerlukan HTTPS untuk semua titik akhir web publik 24
WKLD.14 — Gunakan layanan perlindungan tepi untuk titik akhir publik 25
WKLD.15 - Gunakan template untuk menyebarkan kontrol keamanan 26
Kontributor 27
Riwayat dokumen 28

Glosarium 30
..... 30
A 31
B 34
C 35
D 38
E 42
F 44
G 45
H 46
I 47
L 50
M 51
O 54
P 56
Q 59
R 59
D 62
T 65
U 67
V 67
W 68
Z 69
..... lxx

AWSDasar Keamanan Startup (AWSSSB)

Jay Michael, Layanan Web Amazon (AWS)

Mei 2023(sejarah dokumen)

TheAWSStartup Security Baseline (SSB) adalah seperangkat kontrol yang menciptakan fondasi minimum bagi bisnis untuk membangun dengan amanAWStanpa mengurangi kelincahan mereka. Kontrol ini membentuk dasar dari postur keamanan Anda dan difokuskan pada pengamanan kredensional, memungkinkan pencatatan dan visibilitas, mengelola informasi kontak, dan menerapkan batasan data dasar.

Kontrol dalam panduan ini dirancang dengan mempertimbangkan startup awal, mengurangi risiko keamanan yang paling umum tanpa memerlukan upaya yang signifikan. Banyak startup memulai perjalanan mereka diAWS Clouddengan satuAkun AWS. Seiring pertumbuhan organisasi, mereka bermigrasi ke arsitektur multi-akun. Panduan dalam panduan ini dirancang untuk arsitektur akun tunggal, tetapi membantu Anda mengatur kontrol keamanan yang mudah dimigrasi atau dimodifikasi saat Anda beralih ke arsitektur multi-akun.

Kontrol diAWSSSB dibagi menjadi dua kategori: akun dan beban kerja. Kontrol akun membantu menjagaAWSakun aman. Ini termasuk rekomendasi untuk mengatur akses pengguna, kebijakan, dan izin, dan itu termasuk rekomendasi untuk cara memantau akun Anda untuk aktivitas yang tidak sah atau berpotensi berbahaya. Kontrol beban kerja membantu mengamankan sumber daya dan kode Anda di cloud, seperti aplikasi, proses backend, dan data. Ini termasuk rekomendasi seperti enkripsi dan mengurangi ruang lingkup akses.

> **Note**
>
> Beberapa kontrol yang direkomendasikan dalam panduan ini menggantikan default yang dikonfigurasi selama penyiapan awal, sementara sebagian besar mengonfigurasi pengaturan dan kebijakan baru. Dokumen ini sama sekali tidak boleh dianggap komprehensif dari semua kontrol yang tersedia.

Audiens yang dituju

Panduan ini paling cocok untuk startup yang berada di tahap awal pengembangan, dengan staf dan operasi minimal.

Startup atau bisnis lain yang berada dalam tahap operasi dan pertumbuhan selanjutnya masih dapat memperoleh nilai yang signifikan dari meninjau kontrol ini terhadap praktik mereka saat ini. Jika Anda mengidentifikasi celah, Anda dapat menerapkan kontrol individu dalam panduan ini dan kemudian mengevaluasinya untuk kesesuaian sebagai solusi jangka panjang.

> **Note**
>
> Kontrol yang direkomendasikan dalam panduan ini bersifat mendasar. Startup atau perusahaan lain yang beroperasi pada tahap skala atau kecanggihan selanjutnya harus menambahkan kontrol tambahan sebagaimana berlaku.

Kerangka dasar dan tanggung jawab keamanan

AWSDiarsiteksikan dengan baikmembantu arsitek cloud membangun infrastruktur yang aman, berkinerja tinggi, tangguh, dan efisien untuk aplikasi dan beban kerja mereka. TheAWSStartup Security Baseline sejalan denganpilar keamanandariAWSKerangka Kerja yang Dirancang dengan Baik. Thepilar keamananmenjelaskan cara memanfaatkan teknologi cloud untuk melindungi data, sistem, dan aset dengan cara yang dapat meningkatkan postur keamanan Anda. Ini membantu Anda memenuhi persyaratan bisnis dan peraturan Anda dengan mengikuti saat iniAWSrekomendasi.

Anda dapat menilai kepatuhan Anda terhadap praktik terbaik yang Dirancang dengan Baik dengan menggunakanAWS Well-Architected Tooldalam dirimuAWSakun.

Keamanan dan kepatuhan adalah tanggung jawab bersama antaraAWSdan pelanggan. Themodel tanggung jawab bersamasering digambarkan dengan mengatakan bahwaAWSbertanggung jawab atas keamanan cloud (yaitu, untuk melindungi infrastruktur yang menjalankan semua layanan yang ditawarkan diAWS Cloud), dan Anda bertanggung jawab atas keamanan di cloud (sebagaimana ditentukan olehAWS Cloudlayanan yang Anda pilih). Dalam model tanggung jawab bersama, menerapkan kontrol keamanan dalam dokumen ini adalah bagian dari tanggung jawab Anda sebagai pelanggan.

Mengamankan akun Anda

Kontrol dan rekomendasi di bagian ini membantu menjaga keamanan AWS akun Anda. Ini menekankan penggunaan AWS Identity and Access Management (IAM) pengguna, kelompok pengguna, dan peran (juga dikenal sebagai prinsipal) untuk akses manusia dan mesin, membatasi penggunaan pengguna root, dan membutuhkan otentikasi multi-faktor. Di bagian ini, Anda mengonfirmasi bahwa AWS memiliki informasi kontak yang diperlukan untuk menghubungi Anda mengenai aktivitas dan status akun Anda. Anda juga menyiapkan layanan pemantauan, seperti, Amazon AWS Trusted Advisor, dan GuardDuty AWS Budgets, sehingga Anda diberi tahu tentang aktivitas di akun Anda dan dapat merespons dengan cepat jika aktivitas tersebut tidak sah atau tidak terduga.

Bagian ini berisi topik berikut:

- ACCT.01 - Tetapkan kontak tingkat akun ke daftar distribusi email yang valid
- ACCT.02 — Batasi penggunaan pengguna root
- ACCT.03 - Konfigurasikan akses konsol untuk setiap pengguna
- ACCT.04 - Tetapkan izin
- ACCT.05 — Memerlukan otentikasi multi-faktor (MFA) untuk masuk
- ACCT.06 — Menegakkan kebijakan kata sandi
- ACCT.07 — Mengirimkan CloudTrail log ke bucket S3 yang dilindungi
- ACCT.08 — Mencegah akses publik ke bucket S3 pribadi
- ACCT.09 - Hapus VPC, subnet, dan grup keamanan yang tidak digunakan
- ACCT.10 — Konfigurasi AWS Budgets untuk memantau pengeluaran Anda
- ACCT.11 - Aktifkan dan tanggapi pemberitahuan GuardDuty
- ACCT.12 — Memantau dan menyelesaikan masalah berisiko tinggi dengan menggunakan Trusted Advisor

ACCT.01 - Tetapkan kontak tingkat akun ke daftar distribusi email yang valid

Saat menyiapkan kontak utama dan alternatif untuk AWS akun Anda, gunakan daftar distribusi email, bukan alamat email individu. Menggunakan daftar distribusi email memastikan bahwa kepemilikan dan jangkauan dipertahankan saat individu di organisasi Anda datang dan pergi. Tetapkan kontak

alternatif untuk pemberitahuan penagihan, operasi, dan keamanan, dan gunakan daftar distribusi email yang sesuai. AWS menggunakan alamat email ini untuk menghubungi Anda, jadi penting bagi Anda untuk tetap mengaksesnya.

Untuk mengedit nama akun Anda, kata sandi pengguna akar, dan alamat email pengguna akar

1. Masuk ke halaman Pengaturan Akun di konsol https://console.aws.amazon.com/billing/home?#/account Billing and Cost Management di.
2. Pada halaman Pengaturan Akun, di sampingPengaturan Akun, memilih Mengedit.
3. Di samping bidang yang ingin Anda perbarui, pilih Edit.
4. Setelah Anda memasukkan perubahan, memilih Simpan perubahan.
5. Setelah Anda selesai membuat semua perubahan, memilih Selesai.

Untuk mengedit informasi kontak Anda

1. Pada halaman Pengaturan Akun, di bawah Informasi Kontak, pilih Edit.
2. Untuk bidang yang ingin Anda ubah, masukkan informasi terbaru Anda, lalu pilih Perbarui.

Untuk menambahkan, memperbarui, atau menghapus kontak alternatif

1. Pada halaman Pengaturan Akun, di bawah Kontak Alternatif, pilih Edit.
2. Untuk bidang yang ingin Anda ubah, masukkan informasi terbaru Anda, lalu pilih Perbarui.

ACCT.02 — Batasi penggunaan pengguna root

Pengguna root dibuat saat Anda mendaftar untuk AWS akun, dan pengguna ini memiliki hak kepemilikan penuh dan izin atas akun yang tidak dapat diubah. Hanya gunakan pengguna root untuk tugas-tugas tertentu yang membutuhkannya. Untuk informasi selengkapnya, lihat Tugas yang memerlukan kredensi pengguna root ()AWS Account Management. Lakukan semua tindakan lain di akun Anda dengan menggunakan jenis identitas IAM lainnya, seperti pengguna gabungan dengan peran IAM. Untuk informasi selengkapnya, lihat kredensil AWS keamanan (dokumentasi IAM).

Untuk membatasi penggunaan pengguna root

1. Memerlukan otentikasi multi-faktor (MFA) untuk pengguna root seperti yang dijelaskan dalam. ACCT.05 — Memerlukan otentikasi multi-faktor (MFA) untuk masuk

2. Buat pengguna administratif sehingga Anda tidak menggunakan pengguna root untuk tugas sehari-hari. Untuk informasi selengkapnya tentang mengonfigurasi akses pengguna, lihatACCT.03 - Konfigurasikan akses konsol untuk setiap pengguna.

ACCT.03 - Konfigurasikan akses konsol untuk setiap pengguna

Sebagai praktik terbaik, AWS merekomendasikan penggunaan kredensil sementara untuk memberikan akses Akun AWS dan sumber daya. Kredensi sementara memiliki masa pakai yang terbatas, jadi Anda tidak perlu memutarnya atau mencabutnya secara eksplisit saat tidak lagi diperlukan. Untuk informasi selengkapnya, lihat Kredensial keamanan sementara (dokumentasi IAM).

Untuk pengguna manusia, AWS rekomendasikan untuk menggunakan identitas federasi dari penyedia identitas terpusat (iDP), seperti, Okta, Active Directory AWS IAM Identity Center, atau Ping Identity. Pengguna federasi memungkinkan Anda menentukan identitas di satu lokasi terpusat, dan pengguna dapat mengautentikasi dengan aman ke beberapa aplikasi dan situs web, termasuk AWS, hanya dengan menggunakan satu set kredensil. Untuk informasi lebih lanjut, lihat Federasi identitas di AWS dan Pusat Identitas IAM (AWS situs web).

> **Note**
>
> Federasi identitas dapat mempersulit transisi dari arsitektur akun tunggal ke arsitektur multi-akun. Adalah umum bagi startup untuk menunda implementasi federasi identitas sampai mereka telah membentuk arsitektur multi-akun yang dikelola. AWS Organizations

Untuk mengatur federasi identitas

1. Jika Anda menggunakan Pusat Identitas IAM, lihat Memulai (dokumentasi Pusat Identitas IAM).

   Jika Anda menggunakan iDP eksternal atau pihak ketiga, lihat Membuat penyedia identitas IAM (dokumentasi IAM).
2. Pastikan bahwa IDP Anda memberlakukan otentikasi multi-faktor (MFA).
3. Terapkan izin sesuai dengan. ACCT.04 - Tetapkan izin

Untuk startup yang tidak siap untuk mengkonfigurasi federasi identitas, Anda dapat membuat pengguna langsung di IAM. Ini bukan praktik terbaik keamanan yang direkomendasikan karena ini adalah kredensil jangka panjang yang tidak pernah kedaluwarsa. Namun, ini adalah praktik umum

untuk startup dalam operasi awal untuk mencegah kesulitan transisi ke arsitektur multi-akun ketika mereka siap secara operasional.

Sebagai baseline, Anda dapat membuat pengguna IAM untuk setiap orang yang perlu mengakses. AWS Management Console Jika Anda mengonfigurasi pengguna IAM, jangan bagikan kredensil di seluruh pengguna, dan putar kredenal jangka panjang secara teratur.

> **Warning**
>
> Pengguna IAM memiliki kredensi jangka panjang, yang menghadirkan risiko keamanan. Untuk membantu mengurangi risiko ini, kami menyarankan agar Anda memberikan pengguna ini hanya izin yang mereka perlukan untuk melakukan tugas dan menghapus pengguna ini ketika mereka tidak lagi diperlukan.

Untuk membuat pengguna IAM

1. Buat pengguna IAM (dokumentasi IAM).
2. Terapkan izin sesuai dengan. ACCT.04 - Tetapkan izin

ACCT.04 - Tetapkan izin

Konfigurasikan izin pengguna di akun dengan menetapkan kebijakan ke identitas IAM mereka (grup pengguna atau peran). Anda dapat menyesuaikan izin, atau Anda dapat melampirkan kebijakan AWS terkelola, yang merupakan kebijakan mandiri yang dirancang AWS untuk memberikan izin bagi banyak kasus penggunaan umum. Jika Anda menyesuaikan izin, ikuti praktik terbaik keamanan untuk memberikan hak istimewa paling sedikit. Keistimewaan paling sedikit adalah praktik pemberian izin minimum yang dibutuhkan setiap pengguna untuk melakukan tugas mereka.

Jika Anda menggunakan identitas federasi, pengguna mengakses akun dengan mengasumsikan peran IAM melalui penyedia identitas eksternal. Peran IAM menentukan pengguna yang diautentikasi oleh idP organisasi Anda yang diizinkan untuk dilakukan. AWS Anda menerapkan kebijakan khusus atau AWS terkelola ke peran ini untuk mengonfigurasi izin.

Untuk menetapkan izin untuk identitas federasi

- Jika Anda menggunakan Pusat Identitas IAM, lihat Menggunakan kebijakan IAM dalam kumpulan izin (dokumentasi Pusat Identitas IAM).

Jika Anda menggunakan iDP eksternal atau pihak ketiga, lihat Menambahkan izin identitas IAM (dokumentasi IAM).

Jika Anda menggunakan pengguna IAM, Anda dapat menggunakan grup pengguna atau peran untuk mengelola izin untuk beberapa pengguna IAM. Kami merekomendasikan grup pengguna untuk startup karena mereka lebih mudah dikelola dan tidak terlalu rentan terhadap kesalahan konfigurasi yang dapat menimbulkan risiko keamanan bagi akun Anda. Tetapkan pengguna ke grup pengguna berdasarkan fungsi pekerjaan mereka. Contoh kelompok pengguna termasuk insinyur aplikasi, data, jaringan, dan Operasi Pengembangan (DevOps). Anda juga dapat membagi tipe pengguna menjadi kelompok pengguna yang lebih kecil berdasarkan otoritas pengambilan keputusan, seperti untuk insinyur senior atau non-senior.

Untuk menetapkan izin bagi pengguna IAM

1. Buat grup pengguna IAM (dokumentasi IAM).
2. Lampirkan kebijakan AWS terkelola ke grup pengguna IAM (dokumentasi IAM).

ACCT.05 — Memerlukan otentikasi multi-faktor (MFA) untuk masuk

Dengan MFA, pengguna memiliki perangkat yang menghasilkan respons terhadap tantangan autentikasi. Setiap kredensi pengguna dan respons yang dihasilkan perangkat diperlukan untuk menyelesaikan proses masuk. Sebagai praktik terbaik keamanan, aktifkan MFA untuk Akun AWS akses, terutama untuk kredensil jangka panjang seperti pengguna root akun dan pengguna IAM.

Untuk mengatur MFA untuk pengguna root

1. Masuk ke AWS Management Console athttps://console.aws.amazon.com/.
2. Di sisi kanan bilah navigasi, pilih nama akun Anda, lalu pilih Kredensial Keamanan Saya.
3. Jika perlu, pilih Lanjutkan ke Kredensial Keamanan.
4. Perluas bagian Multi-Factor Authentication (MFA).
5. Pilih Aktifkan MFA.
6. Ikuti petunjuk wizard untuk mengonfigurasi perangkat MFA Anda sesuai dengan itu. Untuk informasi selengkapnya, lihat Mengaktifkan perangkat MFA untuk pengguna AWS di (dokumentasi IAM).

Untuk mengatur MFA di Pusat Identitas IAM

- Aktifkan MFA (dokumentasi Pusat Identitas IAM)

Untuk mengatur MFA untuk pengguna IAM Anda sendiri

1. Dengan menggunakan kredenal masuk Anda, masuk ke konsol IAM di. https://console.aws.amazon.com/iam
2. Di bilah navigasi di kanan atas, pilih nama pengguna Anda, dan kemudian pilih Kredensial Keamanan Saya.
3. Pada tab Kredensial AWS IAM, di bagian Autentikasi multi-faktor, pilih Kelola perangkat MFA.

Untuk mengatur MFA untuk pengguna IAM lainnya

1. Masuk ke AWS Management Console dan buka konsol IAM dihttps://console.aws.amazon.com/iam.
2. Di panel navigasi, pilih Pengguna.
3. Pilih nama pengguna yang ingin Anda aktifkan MFAnya, lalu pilih tab Kredensial IT.
4. Di samping Perangkat MFA yang ditugaskan, pilih Kelola.
5. Ikuti petunjuk wizard untuk mengonfigurasi perangkat MFA Anda sesuai dengan itu. Untuk informasi selengkapnya, lihat Mengaktifkan perangkat MFA untuk pengguna AWS di (dokumentasi IAM).

ACCT.06 — Menegakkan kebijakan kata sandi

Pengguna masuk ke AWS Management Console dengan memberikan kredensi masuk, dan MFA direkomendasikan. Mengharuskan kata sandi mematuhi kebijakan kata sandi yang kuat untuk membantu mencegah penemuan melalui kekerasan atau rekayasa sosial.

Untuk informasi selengkapnya tentang rekomendasi terbaru untuk kata sandi yang kuat, lihat Panduan Kebijakan Kata Sandi di situs web Center for Internet Security (CIS).

Untuk pengguna IAM, Anda dapat mengonfigurasi persyaratan kata sandi dalam kebijakan kata sandi IAM khusus. Untuk informasi selengkapnya, lihat Menyetel kebijakan kata sandi akun (dokumentasi IAM).

Untuk membuat kebijakan kata sandi khusus

1. Masuk ke AWS Management Console dan buka konsol IAM dihttps://console.aws.amazon.com/iam.
2. Di panel navigasi, pilih Pengaturan akun.
3. Di bagian Kebijakan kata sandi, pilih Ubah kebijakan kata sandi.
4. Pilih opsi yang ingin Anda terapkan pada kebijakan kata sandi, lalu pilih Simpan perubahan.

ACCT.07 — Mengirimkan CloudTrail log ke bucket S3 yang dilindungi

Tindakan yang diambil oleh pengguna, peran, dan layanan di AWS akun Anda dicatat sebagai peristiwa di AWS CloudTrail. CloudTrail diaktifkan secara default, dan di CloudTrail konsol, Anda dapat mengakses 90 hari informasi riwayat acara. Untuk melihat, mencari, mengunduh, mengarsipkan, menganalisis, dan menanggapi aktivitas akun di seluruh AWS infrastruktur Anda, lihat Melihat peristiwa dengan riwayat CloudTrail Acara (CloudTrail dokumentasi).

Untuk menyimpan CloudTrail riwayat lebih dari 90 hari dengan data tambahan, Anda membuat jejak baru yang mengirimkan file log ke bucket Amazon Simple Storage Service (Amazon S3) untuk semua jenis peristiwa. Saat membuat jejak di CloudTrail konsol, Anda membuat jejak multi-wilayah.

Untuk membuat jejak yang mengirimkan log untuk semua Wilayah AWS ke bucket S3

1. Buat jejak (CloudTrail dokumentasi). Pada halaman Pilih peristiwa log, lakukan hal berikut:
    a. Untuk aktivitas API, pilih Baca dan Tulis.
    b. Untuk lingkungan praproduksi, pilih Kecualikan AWS KMS peristiwa. Ini mengecualikan semua AWS Key Management Service (AWS KMS) peristiwa dari jejak Anda. AWS KMS membaca tindakan seperti`Encrypt`,`Decrypt`, dan `GenerateDataKey` dapat menghasilkan volume besar peristiwa.

        Untuk lingkungan produksi, pilih untuk mencatat peristiwa manajemen Tulis, dan kosongkan kotak centang untuk Kecualikan AWS KMS peristiwa. Ini tidak termasuk peristiwa AWS KMS baca volume tinggi tetapi masih mencatat peristiwa penulisan yang relevan, seperti, `DisableDelete`, dan. `ScheduleKey` Ini adalah pengaturan AWS KMS pencatatan minimum yang disarankan untuk lingkungan produksi.

2. Jejak baru muncul di halaman Trails. Dalam waktu sekitar 15 menit, CloudTrail menerbitkan file log yang menunjukkan panggilan antarmuka pemrograman AWS aplikasi (API) yang dibuat di akun Anda. Anda dapat melihat file log di bucket S3 yang Anda tentukan.

Untuk membantu mengamankan bucket S3 tempat Anda menyimpan file log CloudTrail

1. Tinjau kebijakan bucket Amazon S3 (CloudTrail dokumentasi) untuk setiap dan semua bucket tempat Anda menyimpan file log dan sesuaikan sesuai kebutuhan untuk menghapus akses yang tidak perlu.
2. Sebagai praktik keamanan terbaik, pastikan untuk menambahkan kunci `aws:SourceArn` kondisi secara manual ke kebijakan bucket. Untuk informasi selengkapnya, lihat Membuat atau memperbarui bucket Amazon S3 yang akan digunakan untuk menyimpan file log untuk jejak organisasi (CloudTrail dokumentasi).
3. Aktifkan MFA Delete (dokumentasi Amazon S3).

ACCT.08 — Mencegah akses publik ke bucket S3 pribadi

Secara default, hanya pengguna root Akun AWS dan prinsipal IAM, jika digunakan, memiliki izin untuk membaca dan menulis ke bucket Amazon S3 yang dibuat oleh prinsipal tersebut. Prinsipal IAM tambahan diberikan akses dengan menggunakan kebijakan berbasis identitas, dan kondisi akses dapat diberlakukan dengan menggunakan kebijakan bucket. Anda dapat membuat kebijakan bucket yang memberikan akses publik umum ke bucket, ember publik.

Bucket yang dibuat pada atau setelah 28 April 2023 mengaktifkan pengaturan Blokir Akses Publik secara default. Untuk bucket yang dibuat sebelum tanggal ini, pengguna mungkin salah mengonfigurasi kebijakan bucket dan secara tidak sengaja memberikan akses ke publik. Anda dapat mencegah kesalahan konfigurasi ini dengan mengaktifkan pengaturan Blokir Akses Publik untuk setiap bucket. Jika Anda tidak memiliki kasus penggunaan saat ini atau masa depan untuk bucket S3 publik, aktifkan pengaturan ini di Akun AWS level tersebut. Setelan ini mencegah kebijakan yang mengizinkan akses publik.

Untuk mencegah akses publik ke bucket S3

- Konfigurasikan blokir setelan akses publik untuk bucket S3 Anda (dokumentasi Amazon S3).

AWS Trusted Advisor menghasilkan temuan kuning untuk bucket S3 yang memungkinkan daftar atau akses baca ke publik dan menghasilkan temuan merah untuk ember yang memungkinkan unggahan atau penghapusan publik. Sebagai garis dasar, ikuti kontrol ACCT.12 — Memantau dan menyelesaikan masalah berisiko tinggi dengan menggunakan Trusted Advisor untuk mengidentifikasi dan memperbaiki bucket yang salah konfigurasi. Bucket S3 yang dapat diakses publik juga ditunjukkan di konsol Amazon S3.

ACCT.09 - Hapus VPC, subnet, dan grup keamanan yang tidak digunakan

Untuk mengurangi kemungkinan masalah keamanan, hapus atau matikan sumber daya apa pun yang tidak digunakan. Di AWS akun baru, secara default virtual private cloud (VPC) dibuat secara otomatis di setiap akun Wilayah AWS, yang memungkinkan Anda menetapkan alamat IP publik di subnet publik. Namun, jika VPC ini tidak diperlukan, ini menimbulkan risiko paparan sumber daya yang tidak diinginkan.

Jika tidak digunakan, hapus VPC default di semua Wilayah, bukan hanya yang ada di Wilayah tempat Anda dapat menerapkan beban kerja. Menghapus VPC juga menghapus komponennya, seperti subnet dan grup keamanan.

> **Note**
>
> Anda dapat melihat semua Wilayah dan VPC di konsol Amazon EC2 Global View di. https://console.aws.amazon.com/ec2globalview/home Untuk informasi selengkapnya, lihat Daftar dan filter sumber daya di seluruh Wilayah menggunakan Tampilan Global Amazon EC2 (dokumentasi Amazon EC2).

Untuk menghapus VPC default yang tidak digunakan

1. Hapus VPC Anda (dokumentasi Amazon VPC).
2. Ulangi sesuai kebutuhan untuk VPC di Wilayah lain.

ACCT.10 — Konfigurasi AWS Budgets untuk memantau pengeluaran Anda

AWS Budgets memungkinkan pemantauan biaya bulanan dan penggunaan dengan pemberitahuan ketika biaya diperkirakan melebihi ambang batas target. Pemberitahuan biaya yang diperkirakan dapat memberikan indikasi aktivitas tak terduga, memberikan pertahanan ekstra selain sistem pemantauan lainnya, seperti AWS Trusted Advisor dan Amazon GuardDuty. Memantau dan memahami AWS biaya Anda juga merupakan bagian dari kebersihan operasional yang baik.

Untuk mengatur anggaran di AWS Budgets

- Buat anggaran biaya (AWS Budgets dokumentasi).

ACCT.11 - Aktifkan dan tanggapi pemberitahuan GuardDuty

Amazon GuardDuty adalah layanan pendeteksi ancaman yang terus memantau perilaku berbahaya atau tidak sah untuk membantu melindungi AWS akun, beban kerja, dan data Anda. Ketika mendeteksi aktivitas yang tidak terduga dan berpotensi berbahaya, GuardDuty memberikan temuan keamanan terperinci untuk visibilitas dan remediasi. GuardDuty dapat mendeteksi ancaman seperti aktivitas penambangan cryptocurrency, akses dari klien dan relay Tor, perilaku tak terduga, dan kredensi IAM yang dikompromikan. Aktifkan GuardDuty dan tanggapi temuan untuk menghentikan perilaku yang berpotensi berbahaya atau tidak sah di AWS lingkungan Anda. Untuk informasi lebih lanjut tentang temuan di GuardDuty, lihat Menemukan jenis (GuardDuty dokumentasi).

Anda dapat menggunakan Amazon CloudWatch Events untuk menyiapkan notifikasi otomatis saat GuardDuty membuat temuan atau perubahan temuan. Pertama, Anda menyiapkan topik Amazon Simple Notification Service (Amazon SNS) dan menambahkan titik akhir, atau alamat email, ke topik tersebut. Kemudian, Anda menyiapkan CloudWatch acara untuk GuardDuty temuan, dan aturan acara memberi tahu titik akhir dalam topik Amazon SNS.

Untuk mengaktifkan GuardDuty dan GuardDuty pemberitahuan

1. Aktifkan Amazon GuardDuty (GuardDuty dokumentasi).
2. Buat aturan CloudWatch Acara untuk memberi tahu Anda tentang GuardDuty temuan (GuardDutydokumentasi).

ACCT.12 — Memantau dan menyelesaikan masalah berisiko tinggi dengan menggunakan Trusted Advisor

AWS Trusted Advisor memindai AWS infrastruktur Anda secara pasif untuk masalah berisiko tinggi atau berdampak tinggi yang terkait dengan keamanan, kinerja, biaya, dan keandalan. Ini memberikan informasi rinci tentang sumber daya yang terpengaruh dan rekomendasi remediasi. Untuk daftar lengkap cek dan deskripsi, lihat AWS Trusted Advisor cek referensi (Trusted Advisor dokumentasi).

Meninjau Trusted Advisor temuan secara berulang, dan memulihkan masalah yang diperlukan. Jika Anda memiliki paket AWS Business Support atau Enterprise Support, Anda dapat berlangganan email temuan mingguan. Untuk informasi selengkapnya, lihat Mengatur preferensi notifikasi (AWS Support dokumentasi).

Untuk melihat masalah di Trusted Advisor

- Tinjau setiap kategori cek sesuai dengan petunjuk di Lihat kategori cek (AWS Support dokumentasi). Minimal, kami sarankan untuk meninjau tindakan yang direkomendasikan masalah, yang berwarna merah.

Mengamankan beban kerja Anda

Kontrol dan rekomendasi di bagian ini membantu Anda mengamankan beban kerja yang berjalanAWS, saat Anda sedang membangunnya. Mereka menekankan praktik aman untuk mengelola rahasia aplikasi dan ruang lingkup akses, meminimalkan rute akses ke sumber daya pribadi, dan menggunakan enkripsi untuk melindungi data dalam perjalanan dan saat istirahat.

Bagian ini berisi topik berikut:

- WKLD.01 - Gunakan peran IAM untuk menghitung izin lingkungan
- WKLD.02 — Batasi cakupan penggunaan kredensi dengan izin kebijakan berbasis sumber daya
- WKLD.03 - Gunakan rahasia singkat atau layanan manajemen rahasia
- WKLD.04 - Mencegah rahasia aplikasi agar tidak terungkap
- WKLD.05 — Mendeteksi dan memulihkan rahasia yang terungkap
- WKLD.06 — Gunakan Manajer Sistem alih-alih SSH atau RDP
- WKLD.07 - Log peristiwa data untuk bucket S3 dengan data sensitif
- WKLD.08 - Enkripsi volume Amazon EBS
- WKLD.09 - Enkripsi basis data Amazon RDS
- WKLD.10 - Menyebarkan sumber daya pribadi ke subnet pribadi
- WKLD.11 — Batasi akses jaringan dengan menggunakan grup keamanan
- WKLD.12 - Gunakan titik akhir VPC untuk mengakses layanan yang didukung
- WKLD.13 - Memerlukan HTTPS untuk semua titik akhir web publik
- WKLD.14 — Gunakan layanan perlindungan tepi untuk titik akhir publik
- WKLD.15 - Tentukan kontrol keamanan dalam template dan terapkan dengan menggunakan praktik CI/CD

WKLD.01 - Gunakan peran IAM untuk menghitung izin lingkungan

DiAWS Identity and Access Management(IAM), aperanmewakili sekumpulan izin yang dapat diasumsikan oleh seseorang atau layanan untuk periode waktu yang dapat dikonfigurasi. Menggunakan peran menghilangkan kebutuhan untuk menyimpan atau mengelola kredensyal jangka panjang, secara signifikan mengurangi kemungkinan penggunaan yang tidak diinginkan. Menetapkan peran IAM secara langsung ke instans Amazon Elastic Compute Cloud (Amazon EC2),AWS Fargatetugas dan layanan,AWS Lambdafungsi, dan lainnyaAWSmenghitung layanan

kapan pun didukung. Aplikasi yang menggunakanAWSSDK dan berjalan di lingkungan komputasi ini secara otomatis menggunakan kredensyal peran IAM untuk otentikasi.

Pendekatan dan instruksi untuk menggunakan peran IAM untuk setiap layanan dapat ditemukan diAWSDokumentasiuntuk layanan. Misalnya, lihat yang berikut ini:

- Peran IAM untuk Amazon EC2(Dokumentasi Amazon EC2)
- Peran IAM untuk tugas(Dokumentasi Layanan Kontainer Elastis Amazon)
- Peran eksekusi Lambda(Dokumentasi Lambda)

WKLD.02 — Batasi cakupan penggunaan kredensi dengan izin kebijakan berbasis sumber daya

Kebijakan adalah objek yang dapat menentukan izin atau menentukan kondisi akses. Ada dua jenis kebijakan utama:

- Kebijakan berbasis identitasdilampirkan ke kepala sekolah dan menentukan apa izin kepala sekolah diAWSlingkungan.
- Kebijakan berbasis sumber dayadilampirkan ke sumber daya, seperti bucket Amazon Simple Storage Service (Amazon S3), atau titik akhir virtual private cloud (VPC). Kebijakan ini menentukan prinsip mana yang diizinkan mengakses, tindakan yang didukung, dan kondisi lain yang harus dipenuhi.

Agar prinsipal diizinkan mengakses untuk melakukan tindakan terhadap sumber daya, ia harus memiliki izin yang diberikan dalam kebijakan berbasis identitas dan memenuhi persyaratan kebijakan berbasis sumber daya. Untuk informasi lebih lanjut, lihatKebijakan berbasis identitas dan kebijakan berbasis sumber daya(Dokumentasi IAM).

Kondisi yang disarankan untuk kebijakan berbasis sumber daya meliputi:

- Batasi akses hanya ke prinsipal dalam organisasi tertentu (didefinisikan dalamAWS Organizations) dengan menggunakan`aws:PrincipalOrgID`kondisi.
- Batasi akses ke lalu lintas yang berasal dari titik akhir VPC atau VPC tertentu dengan menggunakan`aws:SourceVpc`atau`aws:SourceVpce`kondisi, masing-masing.
- Izinkan atau tolak lalu lintas berdasarkan alamat IP sumber dengan menggunakan`aws:SourceIp`kondisi.

Berikut ini adalah contoh kebijakan berbasis sumber daya yang menggunakan`aws:PrincipalOrgID`kondisi untuk mengizinkan hanya prinsipal di**<o-xxxxxxxxxxx>**organisasi untuk mengakses**<bucket-name>**Ember S3:

```
{
   "Version":"2012-10-17",
   "Statement":[
     {
       "Sid":"AllowFromOrganization",
       "Effect":"Allow",
       "Principal":"*",
       "Action":"s3:*",
       "Resource":"arn:aws:s3:::<bucket-name>/*",
       "Condition": {
         "StringEquals": {"aws:PrincipalOrgID":"<o-xxxxxxxxxxx>"}
       }
     }
   ]
}
```

WKLD.03 - Gunakan rahasia singkat atau layanan manajemen rahasia

Rahasia aplikasi sebagian besar terdiri dari kredensyal, seperti pasangan kunci, token akses, sertifikat digital, dan kredensyal masuk. Aplikasi ini menggunakan rahasia ini untuk mendapatkan akses ke layanan lain yang bergantung padanya, seperti database. Untuk membantu melindungi rahasia ini, kami menyarankan agar rahasia tersebut bersifat sementara (dihasilkan pada saat permintaan dan berumur pendek, seperti dengan peran IAM) atau diambil dari layanan manajemen rahasia. Ini mencegah paparan yang tidak disengaja melalui mekanisme yang kurang aman, seperti bertahan dalam file konfigurasi statis. Ini juga membuatnya lebih mudah untuk mempromosikan kode aplikasi dari pengembangan ke lingkungan produksi.

Untuk layanan manajemen rahasia, kami sarankan menggunakan kombinasi Parameter Store, kemampuanAWS Systems Manager, danAWS Secrets Manager:

- Gunakan Parameter Store untuk mengelola rahasia dan parameter lain yang merupakan pasangan nilai kunci individual, berbasis string, panjang keseluruhan pendek, dan sering diakses. Anda menggunakanAWS Key Management Service(AWS KMS) kunci untuk mengenkripsi rahasia. Tidak ada biaya untuk menyimpan parameter di tingkat standar Parameter Store. Untuk informasi

selengkapnya tentang tingkatan parameter, lihat Mengelola tingkatan parameter (dokumentasi Manajer Sistem).

- Gunakan Secrets Manager untuk menyimpan rahasia yang ada dalam bentuk dokumen (seperti beberapa pasangan kunci-nilai terkait), lebih besar dari 4 KB (seperti sertifikat digital), atau akan mendapat manfaat dari rotasi otomatis.

Anda dapat menggunakan Parameter Store API untuk mengambil rahasia yang disimpan di Secrets Manager. Ini memungkinkan Anda untuk membakukan kode dalam aplikasi Anda saat menggunakan kombinasi kedua layanan.

Untuk mengelola rahasia di Parameter Store

1. Buat simetrisAWS KMSkunci(AWS KMSdokumentasi).
2. BuatSecureStringparameter(Dokumentasi Manajer Sistem). Rahasia di Parameter Store menggunakan`SecureString`tipe data.
3. Dalam aplikasi Anda, ambil parameter dari Parameter Store dengan menggunakanAWSSDK untuk bahasa pemrograman Anda. Untuk contoh di Jawa, lihatGetParameter.jawa(Katalog Kode Sampel AWS).

Untuk mengelola rahasia di Secrets Manager

1. Buat rahasia(Dokumentasi Manajer Rahasia).
2. Ambil rahasia dariAWS Secrets Managerdalam kode(Dokumentasi Manajer Rahasia).

   Penting untuk dibacaGunakanAWS Secrets Managerpustaka caching sisi klien untuk meningkatkan ketersediaan dan latensi penggunaan rahasia Anda(AWSposting blog). Menggunakan SDK sisi klien, yang sudah menerapkan praktik terbaik, harus mempercepat dan menyederhanakan penggunaan dan integrasi Secrets Manager.

WKLD.04 - Mencegah rahasia aplikasi agar tidak terungkap

Selama pengembangan lokal, rahasia aplikasi dapat disimpan dalam konfigurasi lokal atau file kode dan secara tidak sengaja diperiksa ke repositori kode sumber. Repositori tidak aman yang dihosting di penyedia layanan publik dapat dikenakan akses tidak sah dan penemuan rahasia ini selanjutnya. Gunakan alat yang tersedia untuk mencegah rahasia diperiksa. Gabungkan pemeriksaan untuk rahasia yang terpapar sebagai bagian dari proses peninjauan kode manual Anda.

Beberapa alat umum yang dapat mencegah rahasia aplikasi diperiksa ke repositori kode sumber adalah:

- Gitleaks(GitHubrepositori)
- Berbisik(GitHubrepositori)
- deteksi-rahasia(GitHubrepositori)
- git-rahasia(GitHubrepositori)
- TruffleHog(GitHubrepositori)

WKLD.05 — Mendeteksi dan memulihkan rahasia yang terungkap

DiWKLD.03 - Gunakan rahasia singkat atau layanan manajemen rahasiadanWKLD.04 - Mencegah rahasia aplikasi agar tidak terungkap, Anda menempatkan langkah-langkah di tempat untuk melindungi rahasia. Dalam kontrol ini, Anda menerapkan solusi yang dapat mendeteksi jika rahasia telah melewati langkah-langkah pencegahan ini, dan Anda dapat memperbaikinya.

AmazonCodeGuruReviewer mendeteksi rahasia aplikasi dalam kode sumber dan menyediakan mekanisme untuk memulihkan dan mempublikasikan rahasia yang terdeteksi di Secrets Manager. Kode aplikasi untuk mengambil rahasia dari Secrets Manager juga disediakan. Lakukan analisis biaya-manfaat untuk menentukan apakah solusi ini tepat untuk bisnis Anda. Sebagai alternatif, beberapa solusi open-source diWKLD.04 - Mencegah rahasia aplikasi agar tidak terungkapmenyediakan kemampuan deteksi untuk rahasia yang ada.

Untuk mengaturCodeGuruIntegrasi reviewer dengan Secrets Manager

- GunakanCodeGuruReviewer untuk mengidentifikasi rahasia hardcode danAWS Secrets Manageruntuk mengamankan mereka(AWSposting blog dan panduan terpandu).

WKLD.06 — Gunakan Manajer Sistem alih-alih SSH atau RDP

Subnet publik, yang memiliki rute default yang menunjuk ke gateway internet, secara inheren merupakan risiko keamanan yang lebih besar daripadasubnet pribadi, mereka yang tidak memiliki rute ke internet. Anda dapat menjalankan instans EC2 di subnet pribadi dan menggunakan kemampuan Manajer SesiAWS Systems Manageruntuk mengakses instance dari jarak jauh melalui salah satuAWS Command Line Interface(AWS CLI) atauAWS Management Console. Anda kemudian dapat menggunakanAWS CLIatau konsol untuk memulai sesi yang terhubung ke instance melalui

terowongan aman, mencegah kebutuhan untuk mengelola kredenal tambahan yang digunakan untuk Secure Shell (SSH) atau protokol desktop jarak jauh Windows (RDP).

Gunakan Session Manager alih-alih menjalankan instans EC2 di subnet publik, menjalankan jump box, atau menjalankan host bastion.

Untuk mengatur Manajer Sesi

1. Pastikan instans EC2 menggunakan sistem operasi terbaru Amazon Machine Images (AMI), seperti Amazon Linux 2 atau Ubuntu. TheAWS Systems ManagerAgen (SSM Agent) sudah diinstal sebelumnya pada AMI.
2. Pastikan instance memiliki konektivitas, baik melalui gateway internet atau melalui titik akhir VPC, ke alamat ini (menggantikan**<region>**dengan yang sesuaiWilayah AWS):
    a. EC2pesan. <region>.amazonaws.com
    b. ssm. <region>.amazonaws.com
    c. ssmmessages. <region>.amazonaws.com
3. LampirkanAWSkebijakan terkelolaAmazonSSMManagedInstanceCoreke peran IAM yang terkait dengan instans Anda.

Untuk informasi lebih lanjut, lihatMenyiapkan Manajer Sesi(Dokumentasi Manajer Sistem).

Untuk memulai sesi

- Memulai sesi(Dokumentasi Manajer Sistem).

WKLD.07 - Log peristiwa data untuk bucket S3 dengan data sensitif

Secara default,AWS CloudTrailmenangkap peristiwa manajemen, peristiwa yang membuat, memodifikasi, atau menghapus sumber daya di akun Anda. Peristiwa manajemen ini tidak menangkap operasi baca atau tulis ke objek individual di bucket Amazon Simple Storage Service. Selama acara keamanan, penting untuk menangkap akses atau penggunaan data yang tidak sah pada catatan individu atau tingkat objek. GunakanCloudTrailuntuk mencatat peristiwa data untuk bucket S3 apa pun yang menyimpan data sensitif atau penting bisnis, untuk tujuan deteksi dan audit.

> **Note**
>
> Biaya tambahan berlaku untuk peristiwa data pencatatan. Untuk informasi selengkapnya, lihat Harga AWS CloudTrail.

Untuk mencatat peristiwa data untuk jejak

1. Masuk keAWS Management Consoledan bukaCloudTrailkonsol dihttps://console.aws.amazon.com/cloudtrail/
2. Di panel navigasi, pilihJalan setapak, dan kemudian pilih nama jejak.
3. DiRincian umum, pilih Edit untuk mengubah pengaturan berikut. Anda tidak dapat mengubah nama jejak.
    a. DiPeristiwa data, pilihSunting.
    b. UntukSumber peristiwa data, pilihS3.
    c. UntukSemua bucket S3 saat ini dan masa depan, jelasMembacadanMenulis.
    d. Dalam pemilihan bucket Individual, telusuri bucket tempat mencatat peristiwa data. Anda dapat memilih beberapa ember di jendela ini. PilihTambahkan emberuntuk mencatat peristiwa data untuk lebih banyak ember. Pilih untuk logMembacaperistiwa, sepertiGetObject,Menulisperistiwa, sepertiPutObject, atau keduanya.
    e. PilihPerbarui jejak.

WKLD.08 - Enkripsi volume Amazon EBS

Menerapkan enkripsi volume Amazon Elastic Block Store (Amazon EBS) sebagai perilaku default diAWSakun. Volume terenkripsi memiliki kinerja operasi input/output per detik (IOPS) yang sama dengan volume yang tidak terenkripsi dengan efek minimal pada latensi. Ini mencegah pembangunan kembali volume di kemudian hari karena kepatuhan atau alasan lain. Untuk informasi lebih lanjut, lihatPraktik terbaik yang harus diketahui untuk enkripsi Amazon EBS(AWSposting blog).

Untuk mengenkripsi volume Amazon EBS

- Aktifkan enkripsi secara default(Dokumentasi Amazon EC2).

WKLD.09 - Enkripsi basis data Amazon RDS

Mirip dengan WKLD.08 - Enkripsi volume Amazon EBS, aktifkan enkripsi database Amazon Relational Database Service (Amazon RDS). Enkripsi ini dilakukan pada tingkat volume yang mendasarinya dan memiliki kinerja IOPS yang sama dengan volume yang tidak terenkripsi dengan efek minimal pada latensi. Untuk informasi lebih lanjut, lihat Ikhtisar mengenkripsi sumber daya Amazon RDS (Dokumentasi Amazon RDS).

Untuk mengenkripsi instance database RDS

- Enkripsi contoh database (Dokumentasi Amazon RDS).

WKLD.10 - Menyebarkan sumber daya pribadi ke subnet pribadi

Menyebarkan sumber daya yang tidak memerlukan akses internet langsung, seperti instans EC2, database, antrian, caching, atau infrastruktur lainnya, ke dalam subnet pribadi VPC. Subnet pribadi tidak memiliki rute yang dinyatakan dalam tabel rute mereka ke gateway internet terlampir dan tidak dapat menerima lalu lintas internet. Lalu lintas yang berasal dari subnet pribadi yang ditujukan untuk internet harus menjalani terjemahan alamat jaringan (NAT) melalui salah satu yang dikelolaAWSNAT Gateway atau instans EC2 yang menjalankan proses NAT di subnet publik. Untuk informasi selengkapnya tentang isolasi jaringan, lihat Keamanan infrastruktur di Amazon VPC (Dokumentasi Amazon VPC).

Gunakan praktik berikut saat membuat sumber daya dan subnet pribadi:

- Saat membuat subnet pribadi, nonaktifkantetapkan alamat IPv4 publik secara otomatis.
- Saat membuat instance EC2 pribadi, nonaktifkanTetapkan IP Publik secara otomatis. Ini mencegah IP publik ditetapkan jika instance secara tidak sengaja disebarkan ke subnet publik melalui kesalahan konfigurasi.

Anda menentukan subnet untuk sumber daya sebagai bagian dari konfigurasinya, bila diperlukan. Anda dapat menerapkan VPC yang mengikuti praktik terbaik menggunakan Arsitektur VPC Modular dan Dapat Diskalakan Mulai Cepat (AWSMulai Cepat).

WKLD.11 — Batasi akses jaringan dengan menggunakan grup keamanan

Gunakan grup keamanan untuk mengontrol lalu lintas ke instans EC2, database RDS, dan sumber daya lain yang didukung. Grup keamanan bertindak sebagai firewall virtual yang dapat diterapkan ke setiap kelompok sumber daya terkait untuk secara konsisten menentukan aturan untuk memungkinkan lalu lintas masuk dan keluar. Selain aturan berdasarkan alamat IP dan port, kelompok keamanan mendukung aturan untuk memungkinkan lalu lintas dari sumber daya yang terkait dengan kelompok keamanan lainnya. Misalnya, grup keamanan database dapat memiliki aturan untuk mengizinkan hanya lalu lintas dari grup keamanan server aplikasi.

Secara default, grup keamanan mengizinkan semua lalu lintas keluar tetapi tidak mengizinkan lalu lintas masuk. Aturan lalu lintas keluar dapat dihapus, atau Anda dapat mengonfigurasi aturan tambahan yang ditambahkan untuk membatasi lalu lintas keluar dan mengizinkan lalu lintas masuk. Jika grup keamanan tidak memiliki aturan keluar, lalu lintas keluar yang berasal dari instans Anda tidak diperbolehkan. Untuk informasi lebih lanjut, lihatKontrol lalu lintas ke sumber daya menggunakan grup keamanan(Dokumentasi Amazon VPC).

Dalam contoh berikut, ada tiga grup keamanan yang mengontrol lalu lintas dari Application Load Balancer ke instans EC2 yang terhubung ke Amazon RDS untuk database MySQL.

Grup keamanan	Aturan-aturan ke dalam	Aturan-aturan ke luar
Grup keamanan Aplikasi Load Balancer	Keterangan:Izinkan lalu lintas HTTPS dari mana saja Jenis:HTTPS Sumber:Di mana-IPv4 (0.0.0.0/0)	Keterangan:Izinkan semua lalu lintas ke mana saja Jenis:Semua lalu lintas Tujuan:Di mana-IPv4 (0.0.0.0/0)
Grup keamanan instans EC2	Keterangan:Izinkan lalu lintas HTTP dari Application Load Balancer Jenis: HTTP	Keterangan:Izinkan semua lalu lintas ke mana saja Jenis:Semua lalu lintas Tujuan:Di mana-IPv4 (0.0.0.0/0)

Grup keamanan	Aturan-aturan ke dalam	Aturan-aturan ke luar
	Sumber:Grup keamanan Aplikasi Load Balancer	
Grup keamanan basis data RDS	Keterangan:Izinkan lalu lintas MySQL dari instans EC2 Jenis:MySQL Sumber:Grup keamanan instans EC2	Tidak ada aturan keluar

WKLD.12 - Gunakan titik akhir VPC untuk mengakses layanan yang didukung

Di VPC, sumber daya yang perlu mengakses AWS atau layanan eksternal lainnya memerlukan rute ke internet (`0.0.0.0/0`) atau ke alamat IP publik dari layanan target. Gunakan titik akhir VPC untuk mengaktifkan rute IP pribadi dari VPC Anda ke dukunganAWSatau layanan lainnya, mencegah kebutuhan untuk menggunakan gateway internet, perangkat NAT, koneksi jaringan pribadi virtual (VPN), atauAWS Direct Connectkoneksi.

Endpoint VPC mendukung melampirkan kebijakan dan grup keamanan untuk mengontrol akses lebih lanjut ke layanan. Misalnya, Anda dapat menulis kebijakan titik akhir VPC untuk Amazon DynamoDB agar hanya mengizinkan tindakan tingkat item dan mencegah tindakan tingkat tabel untuk semua sumber daya di VPC, terlepas dari kebijakan izinnya sendiri. Anda juga dapat menulis kebijakan bucket S3 untuk mengizinkan hanya permintaan yang berasal dari titik akhir VPC tertentu, sehingga menolak semua akses eksternal lainnya. Endpoint VPC juga dapat memiliki aturan grup keamanan yang, misalnya, membatasi akses ke hanya instans EC2 yang terkait dengan grup keamanan khusus aplikasi, seperti tingkat logika bisnis aplikasi web.

Ada berbagai jenis titik akhir VPC. Anda mengakses sebagian besar layanan dengan menggunakan titik akhir antarmuka VPC. DynamoDB diakses menggunakan titik akhir gateway. Amazon S3 mendukung antarmuka dan titik akhir gateway. Titik akhir gateway direkomendasikan untuk beban kerja yang terdapat dalam satuAWSakun dan Wilayah, dan datang tanpa biaya tambahan. Titik akhir antarmuka direkomendasikan jika diperlukan akses yang lebih dapat diperluas, seperti ke bucket S3 dari VPC lain, dari jaringan lokal, atau dari yang berbedaWilayah AWS. Titik akhir antarmuka

dikenakan biaya uptime per jam dan biaya pemrosesan data per GB, yang keduanya lebih rendah dari biaya masing-masing untuk mengirim data ke`0.0.0.0/0`lewatAWSGerbang NAT.

Lihat sumber daya berikut untuk informasi tambahan tentang penggunaan titik akhir VPC:

- Untuk informasi selengkapnya tentang memilih antara titik akhir gateway dan antarmuka untuk Amazon S3, lihatMemilih Strategi Titik Akhir VPC Anda untuk Amazon S3(AWSposting blog).
- Buat titik akhir antarmuka(Dokumentasi Amazon VPC).
- Buat titik akhir gateway(Dokumentasi Amazon VPC).
- Misalnya kebijakan bucket S3 yang membatasi akses ke titik akhir VPC atau VPC tertentu, lihatMembatasi akses ke VPC tertentu(Dokumentasi Amazon S3).
- Misalnya kebijakan titik akhir DynamoDB yang membatasi tindakan, lihatKebijakan titik akhir untuk DynamoDB(Dokumentasi Amazon VPC).

WKLD.13 - Memerlukan HTTPS untuk semua titik akhir web publik

Memerlukan HTTPS untuk memberikan kredibilitas tambahan ke titik akhir web Anda, memungkinkan titik akhir Anda menggunakan sertifikat untuk membuktikan identitasnya, dan mengonfirmasi bahwa semua lalu lintas antara titik akhir Anda dan klien yang terhubung dienkripsi. Untuk situs web publik, ini memberikan manfaat tambahan dari peringkat mesin pencari yang lebih tinggi.

BanyakAWSlayanan menyediakan titik akhir web publik untuk sumber daya Anda, sepertiAWS Elastic Beanstalk, AmazonCloudFront, Amazon API Gateway, Elastic Load Balancing, danAWS Amplify. Untuk petunjuk tentang cara mewajibkan HTTPS untuk masing-masing layanan ini, lihat berikut ini:

- Batang Kacang Elastis(Dokumentasi Beanstalk Elastis)
- CloudFront(CloudFrontdokumentasi)
- Aplikasi Load Balancer(AWSPusat Pengetahuan)
- Penyeimbang Beban Klasik(AWSPusat Pengetahuan)
- Memperkuat(Memperkuat dokumentasi)

Situs web statis yang dihosting di Amazon S3 tidak mendukung HTTPS. Untuk meminta HTTPS untuk situs web ini, Anda dapat menggunakanCloudFront. Akses publik ke bucket S3 yang menyajikan konten melaluiCloudFronttidak diperlukan.

Untuk menggunakanCloudFrontuntuk melayani situs web statis yang dihosting di Amazon S3

1. GunakanCloudFrontuntuk melayani situs web statis yang dihosting di Amazon S3(AWSPusat Pengetahuan).
2. Jika Anda mengonfigurasi akses ke bucket S3 publik,memerlukan HTTPS antara pemirsa danCloudFront(CloudFrontdokumentasi).

   Jika Anda mengonfigurasi akses ke bucket S3 pribadi,membatasi akses ke konten Amazon S3 dengan menggunakan identitas akses asal(CloudFrontdokumentasi).

Selain itu, konfigurasikan titik akhir HTTPS untuk memerlukan protokol dan cipher Transport Layer Security (TLS) modern, kecuali kompatibilitas dengan protokol lama diperlukan. Misalnya, gunakan`ELBSecurityPolicy-FS-1-2-Res-2020-10`atau kebijakan terbaru yang tersedia untuk pendengar HTTPS Application Load Balancer, bukan default`ELBSecurityPolicy-2016-08`. Kebijakan terbaru memerlukan TLS 1.2 minimal, kerahasiaan maju, dan cipher kuat yang kompatibel dengan browser web modern.

Untuk informasi selengkapnya tentang kebijakan keamanan yang tersedia untuk titik akhir publik HTTPS, lihat:

- Kebijakan keamanan SSL yang telah ditentukan sebelumnya untuk Classic Load Balancer(Dokumentasi Penyeimbangan Beban Elastis)
- Kebijakan keamanan untuk Application Load Balancer Anda(Dokumentasi Penyeimbangan Beban Elastis)
- Protokol dan sandi yang didukung antara pemirsa danCloudFront(CloudFrontdokumentasi)

WKLD.14 — Gunakan layanan perlindungan tepi untuk titik akhir publik

Daripada melayani lalu lintas langsung dari layanan komputasi seperti instans atau kontainer EC2, gunakan layanan perlindungan tepi. Ini memberikan lapisan keamanan tambahan antara lalu lintas masuk dari internet dan sumber daya Anda yang melayani lalu lintas itu. Layanan ini dapat memfilter lalu lintas yang tidak diinginkan, menegakkan enkripsi, dan menerapkan perutean atau aturan lain, seperti load balancing, sebelum lalu lintas mencapai sumber daya internal Anda.

AWSLayanan yang dapat memberikan perlindungan endpoint publik meliputiAWS WAF,CloudFront, Elastic Load Balancing, API Gateway, dan Amplify Hosting. Jalankan layanan berbasis VPC, seperti

Elastic Load Balancing, di subnet publik sebagai proxy ke sumber daya layanan web yang berjalan di subnet pribadi.

CloudFront, API Gateway, dan Amazon Route 53 memberikan perlindungan dari serangan Denial of Service (DDoS) Layer 3 dan 4 tanpa biaya, danAWS WAFdapat melindungi terhadap serangan Layer 7.

Petunjuk untuk memulai dengan masing-masing layanan ini dapat ditemukan di sini:

- Memulai denganAWS WAF(AWSsitus web)
- Memulai dengan AmazonCloudFront(CloudFrontdokumentasi)
- Memulai dengan Elastic Load Balancing(Dokumentasi Penyeimbangan Beban Elastis)
- Memulai dengan API Gateway(Dokumentasi API Gateway)
- Memulai dengan Amplify Hosting(Memperkuat dokumentasi)

WKLD.15 - Tentukan kontrol keamanan dalam template dan terapkan dengan menggunakan praktik CI/CD

Infrastruktur sebagai kode(IAc) adalah praktik mendefinisikan semuaAWSsumber daya layanan dan konfigurasi dalam template dan kode yang Anda terapkan dengan menggunakan pipeline continuous integration and continuous delivery (CI/CD), pipeline yang sama yang digunakan untuk menyebarkan aplikasi perangkat lunak. Layanan IAC, sepertiAWS CloudFormation, mendukung kebijakan dan dukungan berbasis identitas IAM dan berbasis sumber dayaAWSLayanan keamanan, seperti AmazonGuardDuty,AWS WAF, dan Amazon VPC. Tangkap artefak ini sebagai template IAc, komit template ke repositori kode sumber, dan kemudian terapkan dengan menggunakan pipeline CI/CD.

Kecuali diperlukan sebaliknya, komit kebijakan izin aplikasi dengan kode aplikasi di repositori yang sama, dan kelola kebijakan sumber daya umum dan konfigurasi layanan keamanan di repositori kode terpisah dan pipeline penerapan.

Untuk informasi lebih lanjut tentang memulai dengan IAc diAWS, lihatAWS Cloud Development Kit (AWS CDK)dokumentasi.

Kontributor

Kontributor dokumen ini meliputi:

- Jay Michael, Arsitek Solusi Utama
- Cole Calistra, Arsitek Solusi Utama
- Justin Plock, Arsitek Solusi Utama
- Faisal Farooq, Arsitek Solusi
- Michael Nguyen, Sr. Arsitek Solusi
- Ritik Khatwani, Arsitek Solusi Sr.
- Paul Hawkins, Kepala Sekolah, Kantor Kepala Petugas Keamanan Informasi (CISO)

Terima kasih khusus kepada orang-orang berikut yang juga membantu dengan bimbingan dan ulasan:

- Robert Taruh
- Mike Sullivan
- Bob Lee III

Riwayat dokumen

Tabel berikut menjelaskan perubahan signifikan pada panduan ini. Jika Anda ingin diberi tahu tentang pembaruan di masa mendatang, Anda dapat berlanggananUmpan RSS.

Perubahan	Deskripsi	Tanggal
Pengaturan bucket Amazon S3	Kami memperbaruiACCT.08 — Mencegah akses publik ke bucket S3 pribadibagian untuk mencerminkan bahwa ember Amazon S3 yang dibuat setelah 28 April 2023 memilikiBlokir Akses Publikpengaturan diaktifkan secara default.	18 Mei 2023
Praktik terbaik keamanan IAM	Kami memperbarui panduan ini untuk penyelarasan dengan yang terbaruAWS Identity and Access Management(IAM) praktik terbaik. Untuk informasi lebih lanjut, lihatPraktik terbaik keamanandalam dokumentasi IAM.	Februari 1, 2023
Peran IAM	Kami menyediakan tautan tambahan keLayanan AWSdokumentasi diWKLD.01 - Gunakan peran IAM untuk menghitung izin lingkungan bagian.	September 22, 2022
Kebijakan kata sandi	Kami memperbarui rekomendasi untuk kata sandi yang kuat untuk menggunakan panduan	Mei 10, 2022

	terbaru dari Pusat Keamanan Internet (CIS).	
Publikasi awal	—	April 13, 2022

AWSGlosarium Panduan Preskriptif

Berikut ini adalah istilah yang umum digunakan dalam strategi, panduan, dan pola yang disediakan oleh Panduan AWS Preskriptif. Untuk menyarankan entri, silakan gunakan tautan Berikan umpan balik di akhir glosarium.

Nomor

7 Rs

Tujuh strategi migrasi umum untuk memindahkan aplikasi ke cloud. Strategi ini dibangun di atas 5 Rs yang diidentifikasi Gartner pada tahun 2011 dan terdiri dari yang berikut:

- Refactor/Re-Architect — Memindahkan aplikasi dan memodifikasi arsitekturnya dengan memanfaatkan sepenuhnya fitur cloud-native untuk meningkatkan kelincahan, kinerja, dan skalabilitas. Ini biasanya melibatkan porting sistem operasi dan database. Contoh: Migrasikan database Oracle lokal Anda ke Amazon Aurora PostgreSQL Compatible Edition.
- Replatform (angkat dan bentuk ulang) — Pindahkan aplikasi ke cloud, dan perkenalkan beberapa tingkat pengoptimalan untuk memanfaatkan kemampuan cloud. Contoh: Migrasikan database Oracle lokal Anda ke Amazon Relational Database Service (Amazon RDS) untuk Oracle di Cloud. AWS
- Pembelian kembali (drop and shop) - Beralih ke produk yang berbeda, biasanya dengan beralih dari lisensi tradisional ke model SaaS. Contoh: Migrasikan sistem manajemen hubungan pelanggan (CRM) Anda ke Salesforce.com.
- Rehost (lift dan shift) — Pindahkan aplikasi ke cloud tanpa membuat perubahan apa pun untuk memanfaatkan kemampuan cloud. Contoh: Migrasikan database Oracle lokal Anda ke Oracle pada instans EC2 di Cloud. AWS
- Relokasi (hypervisor-level lift and shift) — Pindahkan infrastruktur ke cloud tanpa membeli perangkat keras baru, menulis ulang aplikasi, atau memodifikasi operasi yang ada. Skenario migrasi ini khusus untuk VMware Cloud onAWS, yang mendukung kompatibilitas mesin virtual (VM) dan portabilitas beban kerja antara lingkungan lokal Anda dan. AWS Anda dapat menggunakan teknologi VMware Cloud Foundation dari pusat data lokal saat memigrasikan infrastruktur ke VMware Cloud. AWS Contoh: Pindahkan hypervisor yang menghosting database Oracle Anda ke VMware Cloud on. AWS
- Pertahankan (kunjungi kembali) - Simpan aplikasi di lingkungan sumber Anda. Ini mungkin termasuk aplikasi yang memerlukan refactoring besar, dan Anda ingin menunda pekerjaan itu

sampai nanti, dan aplikasi lama yang ingin Anda pertahankan, karena tidak ada pembenaran bisnis untuk memigrasikannya.

- Pensiun — Menonaktifkan atau menghapus aplikasi yang tidak lagi diperlukan di lingkungan sumber Anda.

A

ABAC

Lihat kontrol akses berbasis atribut.

layanan abstrak

Lihat layanan terkelola.

ASAM

Lihat atomisitas, konsistensi, isolasi, daya tahan.

migrasi aktif-aktif

Metode migrasi database di mana database sumber dan target tetap sinkron (dengan menggunakan alat replikasi dua arah atau operasi penulisan ganda), dan kedua database menangani transaksi dari menghubungkan aplikasi selama migrasi. Metode ini mendukung migrasi dalam batch kecil yang terkontrol alih-alih memerlukan pemotongan satu kali. Ini lebih fleksibel tetapi membutuhkan lebih banyak pekerjaan daripada migrasi aktif-pasif.

migrasi aktif-pasif

Metode migrasi database di mana database sumber dan target disimpan dalam sinkron, tetapi hanya database sumber yang menangani transaksi dari menghubungkan aplikasi sementara data direplikasi ke database target. Basis data target tidak menerima transaksi apa pun selama migrasi.

fungsi agregat

Fungsi SQL yang beroperasi pada sekelompok baris dan menghitung nilai pengembalian tunggal untuk grup. Contoh fungsi agregat meliputi `SUM` dan`MAX`.

AI

Lihat kecerdasan buatan.

AIOps

Lihat operasi kecerdasan buatan.

anonimisasi

Proses menghapus informasi pribadi secara permanen dalam kumpulan data. Anonimisasi dapat membantu melindungi privasi pribadi. Data anonim tidak lagi dianggap sebagai data pribadi.

anti-pola

Solusi yang sering digunakan untuk masalah berulang di mana solusinya kontra-produktif, tidak efektif, atau kurang efektif daripada alternatif.

kontrol aplikasi

Pendekatan keamanan yang memungkinkan penggunaan hanya aplikasi yang disetujui untuk membantu melindungi sistem dari malware.

portofolio aplikasi

Kumpulan informasi rinci tentang setiap aplikasi yang digunakan oleh organisasi, termasuk biaya untuk membangun dan memelihara aplikasi, dan nilai bisnisnya. Informasi ini adalah kunci untuk penemuan portofolio dan proses analisis dan membantu mengidentifikasi dan memprioritaskan aplikasi yang akan dimigrasi, dimodernisasi, dan dioptimalkan.

kecerdasan buatan (AI)

Bidang ilmu komputer yang didedikasikan untuk menggunakan teknologi komputasi untuk melakukan fungsi kognitif yang biasanya terkait dengan manusia, seperti belajar, memecahkan masalah, dan mengenali pola. Untuk informasi lebih lanjut, lihat Apa itu Kecerdasan Buatan?

operasi kecerdasan buatan (AIOps)

Proses menggunakan teknik pembelajaran mesin untuk memecahkan masalah operasional, mengurangi insiden operasional dan intervensi manusia, dan meningkatkan kualitas layanan. Untuk informasi selengkapnya tentang cara AIOps digunakan dalam strategi AWS migrasi, lihat panduan integrasi operasi.

enkripsi asimetris

Algoritma enkripsi yang menggunakan sepasang kunci, kunci publik untuk enkripsi dan kunci pribadi untuk dekripsi. Anda dapat berbagi kunci publik karena tidak digunakan untuk dekripsi, tetapi akses ke kunci pribadi harus sangat dibatasi.

atomisitas, konsistensi, isolasi, daya tahan (ACID)

Satu set properti perangkat lunak yang menjamin validitas data dan keandalan operasional database, bahkan dalam kasus kesalahan, kegagalan daya, atau masalah lainnya.

kontrol akses berbasis atribut (ABAC)

Praktik membuat izin berbutir halus berdasarkan atribut pengguna, seperti departemen, peran pekerjaan, dan nama tim. Untuk informasi selengkapnya, lihat ABAC untuk AWS dokumentasi AWS Identity and Access Management (IAM).

sumber data otoritatif

Lokasi di mana Anda menyimpan versi utama data, yang dianggap sebagai sumber informasi yang paling dapat diandalkan. Anda dapat menyalin data dari sumber data otoritatif ke lokasi lain untuk tujuan memproses atau memodifikasi data, seperti menganonimkan, menyunting, atau membuat nama samaran.

Zona Ketersediaan

Lokasi berbeda di dalam Wilayah AWS yang terisolasi dari kegagalan di Availability Zone lainnya dan menyediakan konektivitas jaringan latensi rendah yang murah ke Availability Zone lainnya di Wilayah yang sama.

AWSKerangka Adopsi Cloud (AWSCAF)

Kerangka pedoman dan praktik terbaik AWS untuk membantu organisasi mengembangkan rencana yang efisien dan efektif untuk bergerak dengan sukses ke cloud. AWS CAF mengatur panduan ke dalam enam area fokus yang disebut perspektif: bisnis, orang, tata kelola, platform, keamanan, dan operasi. Perspektif bisnis, orang, dan tata kelola fokus pada keterampilan dan proses bisnis; perspektif platform, keamanan, dan operasi fokus pada keterampilan dan proses teknis. Misalnya, perspektif masyarakat menargetkan pemangku kepentingan yang menangani sumber daya manusia (SDM), fungsi kepegawaian, dan manajemen orang. Untuk perspektif ini, AWS CAF memberikan panduan untuk pengembangan, pelatihan, dan komunikasi orang untuk membantu mempersiapkan organisasi untuk adopsi cloud yang sukses. Untuk informasi lebih lanjut, lihat situs web AWS CAF dan whitepaper AWS CAF.

AWSKerangka Kualifikasi Beban Kerja (AWSWQF)

Alat yang mengevaluasi beban kerja migrasi database, merekomendasikan strategi migrasi, dan memberikan perkiraan kerja. AWS WQF disertakan dengan AWS Schema Conversion Tool ()AWS SCT. Ini menganalisis skema database dan objek kode, kode aplikasi, dependensi, dan karakteristik kinerja, dan memberikan laporan penilaian.

B

BCP

Lihat perencanaan kontinuitas bisnis.

grafik perilaku

Pandangan interaktif yang terpadu tentang perilaku dan interaksi sumber daya dari waktu ke waktu. Anda dapat menggunakan grafik perilaku dengan Amazon Detective untuk memeriksa upaya logon yang gagal, panggilan API yang mencurigakan, dan tindakan serupa. Untuk informasi selengkapnya, lihat Data dalam grafik perilaku di dokumentasi Detektif.

sistem big-endian

Sistem yang menyimpan byte paling signifikan terlebih dahulu. Lihat juga endianness.

klasifikasi biner

Sebuah proses yang memprediksi hasil biner (salah satu dari dua kelas yang mungkin). Misalnya, model ML Anda mungkin perlu memprediksi masalah seperti “Apakah email ini spam atau bukan spam?” atau “Apakah produk ini buku atau mobil?”

filter mekar

Struktur data probabilistik dan efisien memori yang digunakan untuk menguji apakah suatu elemen adalah anggota dari suatu himpunan.

cabang

Area berisi repositori kode. Cabang pertama yang dibuat dalam repositori adalah cabang utama. Anda dapat membuat cabang baru dari cabang yang ada, dan Anda kemudian dapat mengembangkan fitur atau memperbaiki bug di cabang baru. Cabang yang Anda buat untuk membangun fitur biasanya disebut sebagai cabang fitur. Saat fitur siap dirilis, Anda menggabungkan cabang fitur kembali ke cabang utama. Untuk informasi selengkapnya, lihat Tentang cabang (GitHub dokumentasi).

akses break-glass

Dalam keadaan luar biasa dan melalui proses yang disetujui, cara cepat bagi pengguna untuk mendapatkan akses ke Akun AWS yang biasanya tidak memiliki izin untuk mengaksesnya. Untuk informasi lebih lanjut, lihat indikator Implementasikan prosedur break-glass dalam panduan Well-ArchitectedAWS.

strategi brownfield

Infrastruktur yang ada di lingkungan Anda. Saat mengadopsi strategi brownfield untuk arsitektur sistem, Anda merancang arsitektur di sekitar kendala sistem dan infrastruktur saat ini. Jika Anda memperluas infrastruktur yang ada, Anda dapat memadukan strategi brownfield dan greenfield.

cache penyangga

Area memori tempat data yang paling sering diakses disimpan.

kemampuan bisnis

Apa yang dilakukan bisnis untuk menghasilkan nilai (misalnya, penjualan, layanan pelanggan, atau pemasaran). Arsitektur layanan mikro dan keputusan pengembangan dapat didorong oleh kemampuan bisnis. Untuk informasi selengkapnya, lihat bagian Terorganisir di sekitar kemampuan bisnis dari Menjalankan layanan mikro kontainer di whitepaper. AWS

perencanaan kelangsungan bisnis (BCP)

Rencana yang membahas dampak potensial dari peristiwa yang mengganggu, seperti migrasi skala besar, pada operasi dan memungkinkan bisnis untuk melanjutkan operasi dengan cepat.

C

KAFE

Lihat Kerangka Adopsi AWS Cloud.

CCoE

Lihat Cloud Center of Excellence.

CDC

Lihat mengubah pengambilan data.

ubah pengambilan data (CDC)

Proses melacak perubahan ke sumber data, seperti tabel database, dan merekam metadata tentang perubahan tersebut. Anda dapat menggunakan CDC untuk berbagai tujuan, seperti mengaudit atau mereplikasi perubahan dalam sistem target untuk mempertahankan sinkronisasi.

rekayasa kekacauan

Sengaja memperkenalkan kegagalan atau peristiwa yang mengganggu untuk menguji ketahanan sistem. Anda dapat menggunakan AWS Fault Injection Service(AWS FIS) untuk melakukan eksperimen yang menekankan AWS beban kerja Anda dan mengevaluasi responsnya.

CI/CD

Lihat integrasi berkelanjutan dan pengiriman berkelanjutan.

klasifikasi

Proses kategorisasi yang membantu menghasilkan prediksi. Model ML untuk masalah klasifikasi memprediksi nilai diskrit. Nilai diskrit selalu berbeda satu sama lain. Misalnya, model mungkin perlu mengevaluasi apakah ada mobil dalam gambar atau tidak.

Enkripsi sisi klien

Enkripsi data secara lokal, sebelum target Layanan AWS menerimanya.

Cloud Center of Excellence (CCoE)

Tim multi-disiplin yang mendorong upaya adopsi cloud di seluruh organisasi, termasuk mengembangkan praktik terbaik cloud, memobilisasi sumber daya, menetapkan jadwal migrasi, dan memimpin organisasi melalui transformasi skala besar. Untuk informasi selengkapnya, lihat posting CCoE di Blog Strategi AWS Cloud Enterprise.

komputasi cloud

Teknologi cloud yang biasanya digunakan untuk penyimpanan data jarak jauh dan manajemen perangkat IoT. Cloud computing umumnya terhubung ke teknologi edge computing.

model operasi cloud

Dalam organisasi TI, model operasi yang digunakan untuk membangun, mematangkan, dan mengoptimalkan satu atau lebih lingkungan cloud. Untuk informasi selengkapnya, lihat Membangun Model Operasi Cloud Anda.

tahap adopsi cloud

Empat fase yang biasanya dilalui organisasi ketika mereka bermigrasi ke AWS Cloud:

- Proyek — Menjalankan beberapa proyek terkait cloud untuk bukti konsep dan tujuan pembelajaran
- Foundation — Melakukan investasi dasar untuk meningkatkan adopsi cloud Anda (misalnya, membuat landing zone, mendefinisikan CCoE, membuat model operasi)

- Migrasi — Migrasi aplikasi individual
- Re-invention — Mengoptimalkan produk dan layanan, dan berinovasi di cloud

Tahapan ini didefinisikan oleh Stephen Orban dalam posting blog The Journey Toward Cloud-First & the Stages of Adoption di blog AWS Cloud Enterprise Strategy. Untuk informasi tentang bagaimana kaitannya dengan strategi AWS migrasi, lihat panduan kesiapan migrasi.

CMDB

Lihat database manajemen konfigurasi.

repositori kode

Lokasi di mana kode sumber dan aset lainnya, seperti dokumentasi, sampel, dan skrip, disimpan dan diperbarui melalui proses kontrol versi. Repositori cloud umum termasuk GitHub atau. AWS CodeCommit Setiap versi kode disebut cabang. Dalam struktur layanan mikro, setiap repositori dikhususkan untuk satu bagian fungsionalitas. Pipa CI/CD tunggal dapat menggunakan beberapa repositori.

cache dingin

Cache buffer yang kosong, tidak terisi dengan baik, atau berisi data basi atau tidak relevan. Ini mempengaruhi kinerja karena instance database harus membaca dari memori utama atau disk, yang lebih lambat daripada membaca dari cache buffer.

data dingin

Data yang jarang diakses dan biasanya historis. Saat menanyakan jenis data ini, kueri lambat biasanya dapat diterima. Memindahkan data ini ke tingkat atau kelas penyimpanan yang berkinerja lebih rendah dan lebih murah dapat mengurangi biaya.

visi komputer

Bidang AI yang digunakan oleh mesin untuk mengidentifikasi orang, tempat, dan benda dalam gambar dengan akurasi pada atau di atas tingkat manusia. Sering dibangun dengan model pembelajaran mendalam, ini mengotomatiskan ekstraksi, analisis, klasifikasi, dan pemahaman informasi yang berguna dari satu gambar atau urutan gambar.

database manajemen konfigurasi (CMDB)

Repositori yang menyimpan dan mengelola informasi tentang database dan lingkungan TI, termasuk komponen perangkat keras dan perangkat lunak dan konfigurasinya. Anda biasanya menggunakan data dari CMDB dalam penemuan portofolio dan tahap analisis migrasi.

paket kesesuaian

Kumpulan AWS Config aturan dan tindakan remediasi yang dapat Anda kumpulkan untuk menyesuaikan kepatuhan dan pemeriksaan keamanan Anda. Anda dapat menerapkan paket kesesuaian sebagai entitas tunggal di Akun AWS dan Region, atau di seluruh organisasi, dengan menggunakan templat YAMM. Untuk informasi selengkapnya, lihat Paket kesesuaian dalam dokumentasi. AWS Config

integrasi berkelanjutan dan pengiriman berkelanjutan (CI/CD)

Proses mengotomatiskan sumber, membangun, menguji, pementasan, dan tahap produksi dari proses rilis perangkat lunak. CI/CD umumnya digambarkan sebagai pipa. CI/CD dapat membantu Anda mengotomatiskan proses, meningkatkan produktivitas, meningkatkan kualitas kode, dan memberikan lebih cepat. Untuk informasi lebih lanjut, lihat Manfaat pengiriman berkelanjutan. CD juga dapat berarti penerapan berkelanjutan. Untuk informasi selengkapnya, lihat Continuous Delivery vs Continuous Deployment.

D

data saat istirahat

Data yang stasioner di jaringan Anda, seperti data yang ada di penyimpanan.

klasifikasi data

Proses untuk mengidentifikasi dan mengkategorikan data dalam jaringan Anda berdasarkan kekritisan dan sensitivitasnya. Ini adalah komponen penting dari setiap strategi manajemen risiko keamanan siber karena membantu Anda menentukan perlindungan dan kontrol retensi yang tepat untuk data. Klasifikasi data adalah komponen pilar keamanan dalam AWS Well-Architected Framework. Untuk informasi selengkapnya, lihat Klasifikasi data.

penyimpangan data

Variasi yang berarti antara data produksi dan data yang digunakan untuk melatih model ML, atau perubahan yang berarti dalam data input dari waktu ke waktu. Penyimpangan data dapat mengurangi kualitas, akurasi, dan keadilan keseluruhan dalam prediksi model ML.

data dalam transit

Data yang aktif bergerak melalui jaringan Anda, seperti antara sumber daya jaringan.

minimalisasi data

Prinsip pengumpulan dan pemrosesan hanya data yang sangat diperlukan. Mempraktikkan minimalisasi data AWS Cloud dapat mengurangi risiko privasi, biaya, dan jejak karbon analitik Anda.

perimeter data

Satu set pagar pembatas pencegahan di AWS lingkungan Anda yang membantu memastikan bahwa hanya identitas tepercaya yang mengakses sumber daya tepercaya dari jaringan yang diharapkan. Untuk informasi selengkapnya, lihat Membangun perimeter data pada AWS.

prapemrosesan data

Untuk mengubah data mentah menjadi format yang mudah diuraikan oleh model ML Anda. Preprocessing data dapat berarti menghapus kolom atau baris tertentu dan menangani nilai yang hilang, tidak konsisten, atau duplikat.

asal data

Proses melacak asal dan riwayat data sepanjang siklus hidupnya, seperti bagaimana data dihasilkan, ditransmisikan, dan disimpan.

subjek data

Individu yang datanya dikumpulkan dan diproses.

gudang data

Sistem manajemen data yang mendukung intelijen bisnis, seperti analitik. Gudang data biasanya berisi sejumlah besar data historis, dan biasanya digunakan untuk kueri dan analisis.

bahasa definisi database (DDL)

Pernyataan atau perintah untuk membuat atau memodifikasi struktur tabel dan objek dalam database.

bahasa manipulasi basis data (DHTML)

Pernyataan atau perintah untuk memodifikasi (memasukkan, memperbarui, dan menghapus) informasi dalam database.

DDL

Lihat bahasa definisi database.

ansambel yang dalam

Untuk menggabungkan beberapa model pembelajaran mendalam untuk prediksi. Anda dapat menggunakan ansambel dalam untuk mendapatkan prediksi yang lebih akurat atau untuk memperkirakan ketidakpastian dalam prediksi.

pembelajaran mendalam

Subbidang ML yang menggunakan beberapa lapisan jaringan saraf tiruan untuk mengidentifikasi pemetaan antara data input dan variabel target yang diinginkan.

defense-in-depth

Pendekatan keamanan informasi di mana serangkaian mekanisme dan kontrol keamanan dilapisi dengan cermat di seluruh jaringan komputer untuk melindungi kerahasiaan, integritas, dan ketersediaan jaringan dan data di dalamnya. Saat Anda mengadopsi strategi iniAWS, Anda menambahkan beberapa kontrol pada lapisan AWS Organizations struktur yang berbeda untuk membantu mengamankan sumber daya. Misalnya, defense-in-depth pendekatan mungkin menggabungkan otentikasi multi-faktor, segmentasi jaringan, dan enkripsi.

administrator yang didelegasikan

DiAWS Organizations, layanan yang kompatibel dapat mendaftarkan akun AWS anggota untuk mengelola akun organisasi dan mengelola izin untuk layanan tersebut. Akun ini disebut administrator yang didelegasikan untuk layanan itu. Untuk informasi selengkapnya dan daftar layanan yang kompatibel, lihat Layanan yang berfungsi dengan AWS Organizations AWS Organizations dokumentasi.

deployment

Proses pembuatan aplikasi, fitur baru, atau perbaikan kode tersedia di lingkungan target. Deployment melibatkan penerapan perubahan dalam basis kode dan kemudian membangun dan menjalankan basis kode itu di lingkungan aplikasi.

lingkungan pengembangan

Lihat lingkungan.

kontrol detektif

Kontrol keamanan yang dirancang untuk mendeteksi, mencatat, dan memperingatkan setelah suatu peristiwa terjadi. Kontrol ini adalah garis pertahanan kedua, memperingatkan Anda tentang peristiwa keamanan yang melewati kontrol pencegahan di tempat. Untuk informasi selengkapnya, lihat Kontrol Detektif dalam Menerapkan kontrol keamanan pada. AWS

pemetaan aliran nilai pengembangan (DVSM)

Proses yang digunakan untuk mengidentifikasi dan memprioritaskan kendala yang berdampak buruk pada kecepatan dan kualitas dalam siklus hidup pengembangan perangkat lunak. DVSM memperluas proses pemetaan aliran nilai yang awalnya dirancang untuk praktik manufaktur ramping. Ini berfokus pada langkah-langkah dan tim yang diperlukan untuk menciptakan dan memindahkan nilai melalui proses pengembangan perangkat lunak.

kembar digital

Representasi virtual dari sistem dunia nyata, seperti bangunan, pabrik, peralatan industri, atau jalur produksi. Kembar digital mendukung pemeliharaan prediktif, pemantauan jarak jauh, dan optimalisasi produksi.

tabel dimensi

Dalam skema bintang, tabel yang lebih kecil yang berisi atribut data tentang data kuantitatif dalam tabel fakta. Atribut tabel dimensi biasanya bidang teks atau angka diskrit yang berperilaku seperti teks. Atribut ini biasanya digunakan untuk pembatasan kueri, pemfilteran, dan pelabelan set hasil.

musibah

Peristiwa yang mencegah beban kerja atau sistem memenuhi tujuan bisnisnya di lokasi utama yang digunakan. Peristiwa ini dapat berupa bencana alam, kegagalan teknis, atau akibat dari tindakan manusia, seperti kesalahan konfigurasi yang tidak disengaja atau serangan malware.

pemulihan bencana (DR)

Strategi dan proses yang Anda gunakan untuk meminimalkan downtime dan kehilangan data yang disebabkan oleh bencana. Untuk informasi selengkapnya, lihat Disaster Recovery of Workloads onAWS: Recovery in the Cloud in the AWS Well-Architected Framework.

DML~

Lihat bahasa manipulasi database.

desain berbasis domain

Pendekatan untuk mengembangkan sistem perangkat lunak yang kompleks dengan menghubungkan komponennya ke domain yang berkembang, atau tujuan bisnis inti, yang dilayani oleh setiap komponen. Konsep ini diperkenalkan oleh Eric Evans dalam bukunya, Domain-Driven Design: Tackling Complexity in the Heart of Software (Boston: Addison-Wesley Professional, 2003). Untuk informasi tentang cara menggunakan desain berbasis domain dengan pola gambar

pencekik, lihat Memodernisasi layanan web Microsoft ASP.NET (ASMX) lama secara bertahap menggunakan container dan Amazon API Gateway.

DR

Lihat pemulihan bencana.

deteksi drift

Melacak penyimpangan dari konfigurasi dasar. Misalnya, Anda dapat menggunakan AWS CloudFormation untuk mendeteksi penyimpangan dalam sumber daya sistem, atau Anda dapat menggunakannya AWS Control Tower untuk mendeteksi perubahan di landing zone yang mungkin memengaruhi kepatuhan terhadap persyaratan tata kelola.

DVSM

Lihat pemetaan aliran nilai pengembangan.

E

EDA

Lihat analisis data eksplorasi.

komputasi tepi

Teknologi yang meningkatkan daya komputasi untuk perangkat pintar di tepi jaringan IoT. Jika dibandingkan dengan komputasi awan, komputasi tepi dapat mengurangi latensi komunikasi dan meningkatkan waktu respons.

enkripsi

Proses komputasi yang mengubah data plaintext, yang dapat dibaca manusia, menjadi ciphertext.

kunci enkripsi

String kriptografi dari bit acak yang dihasilkan oleh algoritma enkripsi. Panjang kunci dapat bervariasi, dan setiap kunci dirancang agar tidak dapat diprediksi dan unik.

endianness

Urutan byte disimpan dalam memori komputer. Sistem big-endian menyimpan byte paling signifikan terlebih dahulu. Sistem little-endian menyimpan byte paling tidak signifikan terlebih dahulu.

titik akhir

Lihat titik akhir layanan.

layanan endpoint

Layanan yang dapat Anda host di cloud pribadi virtual (VPC) untuk dibagikan dengan pengguna lain. Anda dapat membuat layanan endpoint dengan AWS PrivateLink dan memberikan izin kepada prinsipal lain Akun AWS atau ke AWS Identity and Access Management (IAM). Akun atau prinsipal ini dapat terhubung ke layanan endpoint Anda secara pribadi dengan membuat titik akhir VPC antarmuka. Untuk informasi selengkapnya, lihat Membuat layanan titik akhir di dokumentasi Amazon Virtual Private Cloud (Amazon VPC).

enkripsi amplop

Proses mengenkripsi kunci enkripsi dengan kunci enkripsi lain. Untuk informasi selengkapnya, lihat Enkripsi amplop dalam dokumentasi AWS Key Management Service (AWS KMS).

lingkungan

Sebuah contoh dari aplikasi yang sedang berjalan. Berikut ini adalah jenis lingkungan yang umum dalam komputasi awan:

- Development Environment — Sebuah contoh dari aplikasi yang berjalan yang hanya tersedia untuk tim inti yang bertanggung jawab untuk memelihara aplikasi. Lingkungan pengembangan digunakan untuk menguji perubahan sebelum mempromosikannya ke lingkungan atas. Jenis lingkungan ini kadang-kadang disebut sebagai lingkungan pengujian.
- lingkungan yang lebih rendah — Semua lingkungan pengembangan untuk aplikasi, seperti yang digunakan untuk build awal dan pengujian.
- lingkungan produksi — Sebuah contoh dari aplikasi yang berjalan yang pengguna akhir dapat mengakses. Dalam pipa CI/CD, lingkungan produksi adalah lingkungan penyebaran terakhir.
- lingkungan atas — Semua lingkungan yang dapat diakses oleh pengguna selain tim pengembangan inti. Ini dapat mencakup lingkungan produksi, lingkungan praproduksi, dan lingkungan untuk pengujian penerimaan pengguna.

epik

Dalam metodologi tangkas, kategori fungsional yang membantu mengatur dan memprioritaskan pekerjaan Anda. Epik memberikan deskripsi tingkat tinggi tentang persyaratan dan tugas implementasi. Misalnya, epos keamanan AWS CAF mencakup manajemen identitas dan akses, kontrol detektif, keamanan infrastruktur, perlindungan data, dan respons insiden. Untuk informasi selengkapnya tentang epos dalam strategi AWS migrasi, lihat panduan implementasi program.

analisis data eksplorasi (EDA)

Proses menganalisis dataset untuk memahami karakteristik utamanya. Anda mengumpulkan atau mengumpulkan data dan kemudian melakukan penyelidikan awal untuk menemukan pola, mendeteksi anomali, dan memeriksa asumsi. EDA dilakukan dengan menghitung statistik ringkasan dan membuat visualisasi data.

F

tabel fakta

Tabel tengah dalam skema bintang. Ini menyimpan data kuantitatif tentang operasi bisnis. Biasanya, tabel fakta berisi dua jenis kolom: kolom yang berisi ukuran dan yang berisi kunci asing ke tabel dimensi.

gagal cepat

Filosofi yang menggunakan pengujian yang sering dan bertahap untuk mengurangi siklus hidup pengembangan. Ini adalah bagian penting dari pendekatan tangkas.

batas isolasi kesalahan

DalamAWS Cloud, batas seperti Availability Zone,Wilayah AWS, control plane, atau data plane yang membatasi efek kegagalan dan membantu meningkatkan ketahanan beban kerja. Untuk informasi selengkapnya, lihat Batas Isolasi AWS Kesalahan.

cabang fitur

Lihat cabang.

fitur

Data input yang Anda gunakan untuk membuat prediksi. Misalnya, dalam konteks manufaktur, fitur bisa berupa gambar yang diambil secara berkala dari lini manufaktur.

pentingnya fitur

Seberapa signifikan fitur untuk prediksi model. Ini biasanya dinyatakan sebagai skor numerik yang dapat dihitung melalui berbagai teknik, seperti Shapley Additive Explanations (SHAP) dan gradien terintegrasi. Untuk informasi lebih lanjut, lihat Interpretabilitas model pembelajaran mesin dengan:. AWS

transformasi fitur

Untuk mengoptimalkan data untuk proses ML, termasuk memperkaya data dengan sumber tambahan, menskalakan nilai, atau mengekstrak beberapa set informasi dari satu bidang data. Hal ini memungkinkan model ML untuk mendapatkan keuntungan dari data. Misalnya, jika Anda memecah tanggal “2021-05-27 00:15:37" menjadi “2021", “Mei”, “Kamis”, dan “15", Anda dapat membantu algoritme pembelajaran mempelajari pola bernuansa yang terkait dengan komponen data yang berbeda.

FGAC

Lihat kontrol akses berbutir halus.

kontrol akses berbutir halus (FGAC)

Penggunaan beberapa kondisi untuk mengizinkan atau menolak permintaan akses.

migrasi flash-cut

Metode migrasi database yang menggunakan replikasi data berkelanjutan melalui pengambilan data perubahan untuk memigrasikan data dalam waktu sesingkat mungkin, alih-alih menggunakan pendekatan bertahap. Tujuannya adalah untuk menjaga downtime seminimal mungkin.

G

pemblokiran geografis

Lihat pembatasan geografis.

pembatasan geografis (pemblokiran geografis)

Di Amazon CloudFront, opsi untuk mencegah pengguna di negara tertentu mengakses distribusi konten. Anda dapat menggunakan daftar izinkan atau daftar blokir untuk menentukan negara yang disetujui dan dilarang. Untuk informasi selengkapnya, lihat Membatasi distribusi geografis konten Anda dalam dokumentasi. CloudFront

Alur kerja Gitflow

Pendekatan di mana lingkungan bawah dan atas menggunakan cabang yang berbeda dalam repositori kode sumber. Alur kerja Gitflow dianggap warisan, dan alur kerja berbasis batang adalah pendekatan modern yang disukai.

strategi greenfield

Tidak adanya infrastruktur yang ada di lingkungan baru. Saat mengadopsi strategi greenfield untuk arsitektur sistem, Anda dapat memilih semua teknologi baru tanpa batasan kompatibilitas dengan infrastruktur yang ada, juga dikenal sebagai brownfield. Jika Anda memperluas infrastruktur yang ada, Anda dapat memadukan strategi brownfield dan greenfield.

pagar pembatas

Aturan tingkat tinggi yang membantu mengatur sumber daya, kebijakan, dan kepatuhan di seluruh unit organisasi (OU). Pagar pembatas preventif menegakkan kebijakan untuk memastikan keselarasan dengan standar kepatuhan. Mereka diimplementasikan dengan menggunakan kebijakan kontrol layanan dan batas izin IAM. Detective guardrails mendeteksi pelanggaran kebijakan dan masalah kepatuhan, dan menghasilkan peringatan untuk remediasi. Mereka diimplementasikan dengan menggunakanAWS Config,AWS Security Hub, Amazon GuardDutyAWS Trusted Advisor, Amazon Inspector, dan pemeriksaan khususAWS Lambda.

H

HA

Lihat ketersediaan tinggi.

migrasi database heterogen

Memigrasi database sumber Anda ke database target yang menggunakan mesin database yang berbeda (misalnya, Oracle ke Amazon Aurora). Migrasi heterogen biasanya merupakan bagian dari upaya arsitektur ulang, dan mengubah skema dapat menjadi tugas yang kompleks. AWSmenyediakan AWS SCT yang membantu dengan konversi skema.

ketersediaan tinggi (HA)

Kemampuan beban kerja untuk beroperasi terus menerus, tanpa intervensi, jika terjadi tantangan atau bencana. Sistem HA dirancang untuk gagal secara otomatis, secara konsisten memberikan kinerja berkualitas tinggi, dan menangani beban dan kegagalan yang berbeda dengan dampak kinerja minimal.

modernisasi sejarawan

Pendekatan yang digunakan untuk memodernisasi dan meningkatkan sistem teknologi operasional (OT) untuk melayani kebutuhan industri manufaktur dengan lebih baik. Sejarawan

adalah jenis database yang digunakan untuk mengumpulkan dan menyimpan data dari berbagai sumber di pabrik.

migrasi database homogen

Memigrasi database sumber Anda ke database target yang berbagi mesin database yang sama (misalnya, Microsoft SQL Server ke Amazon RDS for SQL Server). Migrasi homogen biasanya merupakan bagian dari upaya rehosting atau replatforming. Anda dapat menggunakan utilitas database asli untuk memigrasi skema.

data panas

Data yang sering diakses, seperti data real-time atau data translasi terbaru. Data ini biasanya memerlukan tingkat atau kelas penyimpanan berkinerja tinggi untuk memberikan respons kueri yang cepat.

perbaikan terbaru

Perbaikan mendesak untuk masalah kritis dalam lingkungan produksi. Karena urgensinya, perbaikan terbaru biasanya dibuat di luar alur kerja DevOps rilis biasa.

periode hypercare

Segera setelah cutover, periode waktu ketika tim migrasi mengelola dan memantau aplikasi yang dimigrasi di cloud untuk mengatasi masalah apa pun. Biasanya, periode ini panjangnya 1-4 hari. Pada akhir periode hypercare, tim migrasi biasanya mentransfer tanggung jawab untuk aplikasi ke tim operasi cloud.

I

IAc

Lihat infrastruktur sebagai kode.

kebijakan berbasis identitas

Kebijakan yang dilampirkan pada satu atau beberapa prinsip IAM yang mendefinisikan izin mereka dalam lingkungan. AWS Cloud

aplikasi idle

Aplikasi yang memiliki penggunaan CPU dan memori rata-rata antara 5 dan 20 persen selama periode 90 hari. Dalam proyek migrasi, adalah umum untuk menghentikan aplikasi ini atau mempertahankannya di tempat.

IIoT

Lihat Internet of Things industri.

infrastruktur yang tidak dapat diubah

Model yang menyebarkan infrastruktur baru untuk beban kerja produksi alih-alih memperbarui, menambal, atau memodifikasi infrastruktur yang ada. Infrastruktur yang tidak dapat diubah secara inheren lebih konsisten, andal, dan dapat diprediksi daripada infrastruktur yang dapat berubah. Untuk informasi selengkapnya, lihat praktik terbaik Deploy using immutable infrastructure di AWS Well-Architected Framework.

masuk (masuknya) VPC

Dalam arsitektur AWS multi-akun, VPC yang menerima, memeriksa, dan merutekan koneksi jaringan dari luar aplikasi. Arsitektur Referensi AWS Keamanan merekomendasikan pengaturan akun Jaringan Anda dengan VPC masuk, keluar, dan inspeksi untuk melindungi antarmuka dua arah antara aplikasi Anda dan internet yang lebih luas.

migrasi inkremental

Strategi cutover di mana Anda memigrasikan aplikasi Anda dalam bagian-bagian kecil alih-alih melakukan satu cutover penuh. Misalnya, Anda mungkin hanya memindahkan beberapa layanan mikro atau pengguna ke sistem baru pada awalnya. Setelah Anda memverifikasi bahwa semuanya berfungsi dengan baik, Anda dapat secara bertahap memindahkan layanan mikro atau pengguna tambahan hingga Anda dapat menonaktifkan sistem lama Anda. Strategi ini mengurangi risiko yang terkait dengan migrasi besar.

infrastruktur

Semua sumber daya dan aset yang terkandung dalam lingkungan aplikasi.

infrastruktur sebagai kode (IAc)

Proses penyediaan dan pengelolaan infrastruktur aplikasi melalui satu set file konfigurasi. IAc dirancang untuk membantu Anda memusatkan manajemen infrastruktur, menstandarisasi sumber daya, dan menskalakan dengan cepat sehingga lingkungan baru dapat diulang, andal, dan konsisten.

Internet of Things industri (IIoT)

Penggunaan sensor dan perangkat yang terhubung ke internet di sektor industri, seperti manufaktur, energi, otomotif, perawatan kesehatan, ilmu kehidupan, dan pertanian. Untuk

informasi selengkapnya, lihat Membangun strategi transformasi digital Internet of Things (IIoT) industri.

inspeksi VPC

Dalam arsitektur AWS multi-akun, VPC terpusat yang mengelola inspeksi lalu lintas jaringan antara VPC (dalam hal yang sama atau berbedaWilayah AWS), internet, dan jaringan lokal. Arsitektur Referensi AWS Keamanan merekomendasikan pengaturan akun Jaringan Anda dengan VPC masuk, keluar, dan inspeksi untuk melindungi antarmuka dua arah antara aplikasi Anda dan internet yang lebih luas.

Internet of Things (IoT)

Jaringan objek fisik yang terhubung dengan sensor atau prosesor tertanam yang berkomunikasi dengan perangkat dan sistem lain melalui internet atau melalui jaringan komunikasi lokal. Untuk informasi lebih lanjut, lihat Apa itu IoT?

interpretabilitas

Karakteristik model pembelajaran mesin yang menggambarkan sejauh mana manusia dapat memahami bagaimana prediksi model bergantung pada inputnya. Untuk informasi selengkapnya, lihat Interpretabilitas model pembelajaran mesin dengan AWS.

IoT

Lihat Internet of Things.

Perpustakaan informasi TI (ITIL)

Serangkaian praktik terbaik untuk memberikan layanan TI dan menyelaraskan layanan ini dengan persyaratan bisnis. ITIL menyediakan dasar untuk ITSM.

Manajemen layanan TI (ITSM)

Kegiatan yang terkait dengan merancang, menerapkan, mengelola, dan mendukung layanan TI untuk suatu organisasi. Untuk informasi tentang mengintegrasikan operasi cloud dengan alat ITSM, lihat panduan integrasi operasi.

ITIL

Lihat perpustakaan informasi TI.

ITSM

Lihat manajemen layanan TI.

L

kontrol akses berbasis label (LBAC)

Implementasi kontrol akses wajib (MAC) di mana pengguna dan data itu sendiri masing-masing secara eksplisit diberi nilai label keamanan. Persimpangan antara label keamanan pengguna dan label keamanan data menentukan baris dan kolom mana yang dapat dilihat oleh pengguna.

landing zone

Landing zone adalah AWS lingkungan multi-akun yang dirancang dengan baik yang dapat diskalakan dan aman. Ini adalah titik awal dari mana organisasi Anda dapat dengan cepat meluncurkan dan menyebarkan beban kerja dan aplikasi dengan percaya diri dalam lingkungan keamanan dan infrastruktur mereka. Untuk informasi selengkapnya tentang zona pendaratan, lihat Menyiapkan lingkungan multi-akun AWS yang aman dan dapat diskalakan.

migrasi besar

Migrasi 300 atau lebih server.

LBAC

Lihat kontrol akses berbasis label.

hak istimewa paling sedikit

Praktik keamanan terbaik untuk memberikan izin minimum yang diperlukan untuk melakukan tugas. Untuk informasi selengkapnya, lihat Menerapkan izin hak istimewa terkecil dalam dokumentasi IAM.

angkat dan geser

Lihat 7 Rs.

sistem endian kecil

Sistem yang menyimpan byte paling tidak signifikan terlebih dahulu. Lihat juga endianness.

lingkungan yang lebih rendah

Lihat lingkungan.

M

pembelajaran mesin (ML)

Jenis kecerdasan buatan yang menggunakan algoritma dan teknik untuk pengenalan pola dan pembelajaran. ML menganalisis dan belajar dari data yang direkam, seperti data Internet of Things (IoT), untuk menghasilkan model statistik berdasarkan pola. Untuk informasi selengkapnya, lihat Machine Learning.

cabang utama

Lihat cabang.

layanan terkelola

Layanan AWSyang AWS mengoperasikan lapisan infrastruktur, sistem operasi, dan platform, dan Anda mengakses titik akhir untuk menyimpan dan mengambil data. Amazon Simple Storage Service (Amazon S3) dan Amazon DynamoDB adalah contoh layanan terkelola. Ini juga dikenal sebagai layanan abstrak.

PETA

Lihat Program Percepatan Migrasi.

mekanisme

Proses lengkap di mana Anda membuat alat, mendorong adopsi alat, dan kemudian memeriksa hasilnya untuk melakukan penyesuaian. Mekanisme adalah siklus yang memperkuat dan meningkatkan dirinya sendiri saat beroperasi. Untuk informasi lebih lanjut, lihat Membangun mekanisme di AWS Well-Architected Framework.

akun anggota

Semua Akun AWS selain akun manajemen yang merupakan bagian dari organisasi diAWS Organizations. Akun dapat menjadi anggota dari hanya satu organisasi pada suatu waktu.

layanan mikro

Layanan kecil dan independen yang berkomunikasi melalui API yang terdefinisi dengan baik dan biasanya dimiliki oleh tim kecil yang mandiri. Misalnya, sistem asuransi mungkin mencakup layanan mikro yang memetakan kemampuan bisnis, seperti penjualan atau pemasaran, atau subdomain, seperti pembelian, klaim, atau analitik. Manfaat layanan mikro termasuk kelincahan, penskalaan yang fleksibel, penyebaran yang mudah, kode yang dapat digunakan kembali,

dan ketahanan. Untuk informasi selengkapnya, lihat Mengintegrasikan layanan mikro dengan menggunakan layanan tanpa AWS server.

arsitektur microservices

Pendekatan untuk membangun aplikasi dengan komponen independen yang menjalankan setiap proses aplikasi sebagai layanan mikro. Layanan mikro ini berkomunikasi melalui antarmuka yang terdefinisi dengan baik dengan menggunakan API ringan. Setiap layanan mikro dalam arsitektur ini dapat diperbarui, digunakan, dan diskalakan untuk memenuhi permintaan fungsi tertentu dari suatu aplikasi. Untuk informasi selengkapnya, lihat Menerapkan layanan mikro di AWS.

Program Percepatan Migrasi (MAP)

AWSProgram yang menyediakan dukungan konsultasi, pelatihan, dan layanan untuk membantu organisasi membangun fondasi operasional yang kuat untuk pindah ke cloud, dan untuk membantu mengimbangi biaya awal migrasi. MAP mencakup metodologi migrasi untuk mengeksekusi migrasi lama dengan cara metodis dan seperangkat alat untuk mengotomatisasi dan mempercepat skenario migrasi umum.

migrasi dalam skala

Proses memindahkan sebagian besar portofolio aplikasi ke cloud dalam gelombang, dengan lebih banyak aplikasi bergerak pada tingkat yang lebih cepat di setiap gelombang. Fase ini menggunakan praktik terbaik dan pelajaran yang dipetik dari fase sebelumnya untuk mengimplementasikan pabrik migrasi tim, alat, dan proses untuk merampingkan migrasi beban kerja melalui otomatisasi dan pengiriman tangkas. Ini adalah fase ketiga dari strategi AWS migrasi.

pabrik migrasi

Tim lintas fungsi yang merampingkan migrasi beban kerja melalui pendekatan otomatis dan gesit. Tim pabrik migrasi biasanya mencakup operasi, analis dan pemilik bisnis, insinyur migrasi, pengembang, dan DevOps profesional yang bekerja di sprint. Antara 20 dan 50 persen portofolio aplikasi perusahaan terdiri dari pola berulang yang dapat dioptimalkan dengan pendekatan pabrik. Untuk informasi selengkapnya, lihat diskusi tentang pabrik migrasi dan panduan Pabrik Migrasi Cloud di kumpulan konten ini.

metadata migrasi

Informasi tentang aplikasi dan server yang diperlukan untuk menyelesaikan migrasi. Setiap pola migrasi memerlukan satu set metadata migrasi yang berbeda. Contoh metadata migrasi termasuk subnet target, grup keamanan, dan akun. AWS

pola migrasi

Tugas migrasi berulang yang merinci strategi migrasi, tujuan migrasi, dan aplikasi atau layanan migrasi yang digunakan. Contoh: Rehost migrasi ke Amazon EC2 AWS dengan Layanan Migrasi Aplikasi.

Penilaian Portofolio Migrasi (MPA)

Alat online yang menyediakan informasi untuk memvalidasi kasus bisnis untuk bermigrasi ke Cloud. AWS MPA menyediakan penilaian portofolio terperinci (ukuran kanan server, harga, perbandingan TCO, analisis biaya migrasi) serta perencanaan migrasi (analisis data aplikasi dan pengumpulan data, pengelompokan aplikasi, prioritas migrasi, dan perencanaan gelombang). Alat MPA (memerlukan login) tersedia gratis untuk semua AWS konsultan dan konsultan APN Partner.

Penilaian Kesiapan Migrasi (MRA)

Proses mendapatkan wawasan tentang status kesiapan cloud organisasi, mengidentifikasi kekuatan dan kelemahan, dan membangun rencana aksi untuk menutup kesenjangan yang diidentifikasi, menggunakan CAF. AWS Untuk informasi selengkapnya, lihat panduan kesiapan migrasi. MRA adalah tahap pertama dari strategi AWS migrasi.

strategi migrasi

Pendekatan yang digunakan untuk memigrasikan beban kerja ke Cloud. AWS Untuk informasi lebih lanjut, lihat entri 7 Rs di glosarium ini dan lihat Memobilisasi organisasi Anda untuk mempercepat migrasi skala besar.

ML

Lihat pembelajaran mesin.

MPA

Lihat Penilaian Portofolio Migrasi.

modernisasi

Mengubah aplikasi usang (warisan atau monolitik) dan infrastrukturnya menjadi sistem yang gesit, elastis, dan sangat tersedia di cloud untuk mengurangi biaya, mendapatkan efisiensi, dan memanfaatkan inovasi. Untuk informasi selengkapnya, lihat Strategi untuk memodernisasi aplikasi di Cloud. AWS

penilaian kesiapan modernisasi

Evaluasi yang membantu menentukan kesiapan modernisasi aplikasi organisasi; mengidentifikasi manfaat, risiko, dan dependensi; dan menentukan seberapa baik organisasi dapat mendukung

keadaan masa depan aplikasi tersebut. Hasil penilaian adalah cetak biru arsitektur target, peta jalan yang merinci fase pengembangan dan tonggak untuk proses modernisasi, dan rencana aksi untuk mengatasi kesenjangan yang diidentifikasi. Untuk informasi selengkapnya, lihat Mengevaluasi kesiapan modernisasi untuk aplikasi di Cloud. AWS

aplikasi monolitik (monolit)

Aplikasi yang berjalan sebagai layanan tunggal dengan proses yang digabungkan secara ketat. Aplikasi monolitik memiliki beberapa kelemahan. Jika satu fitur aplikasi mengalami lonjakan permintaan, seluruh arsitektur harus diskalakan. Menambahkan atau meningkatkan fitur aplikasi monolitik juga menjadi lebih kompleks ketika basis kode tumbuh. Untuk mengatasi masalah ini, Anda dapat menggunakan arsitektur microservices. Untuk informasi lebih lanjut, lihat Menguraikan monolit menjadi layanan mikro.

klasifikasi multiclass

Sebuah proses yang membantu menghasilkan prediksi untuk beberapa kelas (memprediksi satu dari lebih dari dua hasil). Misalnya, model ML mungkin bertanya “Apakah produk ini buku, mobil, atau telepon?” atau “Kategori produk mana yang paling menarik bagi pelanggan ini?”

infrastruktur yang bisa berubah

Model yang memperbarui dan memodifikasi infrastruktur yang ada untuk beban kerja produksi. Untuk meningkatkan konsistensi, keandalan, dan prediktabilitas, AWS Well-Architected Framework merekomendasikan penggunaan infrastruktur yang tidak dapat diubah sebagai praktik terbaik.

O

OAC

Lihat kontrol akses asal.

OAI

Lihat identitas akses asal.

OCM

Lihat manajemen perubahan organisasi.

migrasi offline

Metode migrasi di mana beban kerja sumber diturunkan selama proses migrasi. Metode ini melibatkan waktu henti yang diperpanjang dan biasanya digunakan untuk beban kerja kecil dan tidak kritis.

OI

Lihat integrasi operasi.

OLA

Lihat perjanjian tingkat operasional.

migrasi online

Metode migrasi di mana beban kerja sumber disalin ke sistem target tanpa diambil offline. Aplikasi yang terhubung ke beban kerja dapat terus berfungsi selama migrasi. Metode ini melibatkan waktu henti nol hingga minimal dan biasanya digunakan untuk beban kerja produksi yang kritis.

perjanjian tingkat operasional (OLA)

Perjanjian yang menjelaskan apa yang dijanjikan kelompok TI fungsional untuk diberikan satu sama lain, untuk mendukung perjanjian tingkat layanan (SLA).

Tinjauan Kesiapan Operasional (ORR)

Daftar pertanyaan dan praktik terbaik terkait yang membantu Anda memahami, mengevaluasi, mencegah, atau mengurangi ruang lingkup insiden dan kemungkinan kegagalan. Untuk informasi lebih lanjut, lihat Ulasan Kesiapan Operasional (ORR) dalam Kerangka Kerja Well-ArchitectedAWS.

integrasi operasi (OI)

Proses modernisasi operasi di cloud, yang melibatkan perencanaan kesiapan, otomatisasi, dan integrasi. Untuk informasi selengkapnya, lihat panduan integrasi operasi.

jejak organisasi

Jejak yang dibuat oleh AWS CloudTrail itu mencatat semua peristiwa untuk semua Akun AWS dalam organisasi diAWS Organizations. Jejak ini dibuat di setiap Akun AWS bagian organisasi dan melacak aktivitas di setiap akun. Untuk informasi selengkapnya, lihat Membuat jejak untuk organisasi dalam CloudTrail dokumentasi.

manajemen perubahan organisasi (OCM)

Kerangka kerja untuk mengelola transformasi bisnis utama yang mengganggu dari perspektif orang, budaya, dan kepemimpinan. OCM membantu organisasi mempersiapkan, dan transisi ke, sistem dan strategi baru dengan mempercepat adopsi perubahan, mengatasi masalah transisi, dan mendorong perubahan budaya dan organisasi. Dalam strategi AWS migrasi, kerangka kerja ini disebut percepatan orang, karena kecepatan perubahan yang diperlukan dalam proyek adopsi cloud. Untuk informasi lebih lanjut, lihat panduan OCM.

kontrol akses asal (OAC)

Di CloudFront, opsi yang disempurnakan untuk membatasi akses untuk mengamankan konten Amazon Simple Storage Service (Amazon S3) Anda. OAC mendukung semua bucket S3 di semuaWilayah AWS, enkripsi sisi server dengan AWS KMS (SSE-KMS), dan dinamis dan permintaan ke bucket S3. `PUT` `DELETE`

identitas akses asal (OAI)

Di CloudFront, opsi untuk membatasi akses untuk mengamankan konten Amazon S3 Anda. Saat Anda menggunakan OAI, CloudFront buat prinsipal yang dapat diautentikasi oleh Amazon S3. Prinsipal yang diautentikasi dapat mengakses konten dalam bucket S3 hanya melalui distribusi tertentu. CloudFront Lihat juga OAC, yang menyediakan kontrol akses yang lebih terperinci dan ditingkatkan.

ORR

Lihat tinjauan kesiapan operasional.

keluar (jalan keluar) VPC

Dalam arsitektur AWS multi-akun, VPC yang menangani koneksi jaringan yang dimulai dari dalam aplikasi. Arsitektur Referensi AWS Keamanan merekomendasikan pengaturan akun Jaringan Anda dengan VPC masuk, keluar, dan inspeksi untuk melindungi antarmuka dua arah antara aplikasi Anda dan internet yang lebih luas.

P

batas izin

Kebijakan manajemen IAM yang dilampirkan pada prinsipal IAM untuk menetapkan izin maksimum yang dapat dimiliki pengguna atau peran. Untuk informasi selengkapnya, lihat Batas izin dalam dokumentasi IAM.

Informasi Identifikasi Pribadi (PII)

Informasi yang, jika dilihat secara langsung atau dipasangkan dengan data terkait lainnya, dapat digunakan untuk menyimpulkan identitas individu secara wajar. Contoh PII termasuk nama, alamat, dan informasi kontak.

PII

Lihat informasi yang dapat diidentifikasi secara pribadi.

buku pedoman

Serangkaian langkah yang telah ditentukan sebelumnya yang menangkap pekerjaan yang terkait dengan migrasi, seperti mengirimkan fungsi operasi inti di cloud. Buku pedoman dapat berupa skrip, runbook otomatis, atau ringkasan proses atau langkah-langkah yang diperlukan untuk mengoperasikan lingkungan modern Anda.

kebijakan

Objek yang dapat menentukan izin (lihat kebijakan berbasis identitas), menentukan kondisi akses (lihat kebijakanberbasis sumber daya), atau menentukan izin maksimum untuk semua akun dalam organisasi di (lihat kebijakan kontrol layanan). AWS Organizations

ketekunan poliglot

Secara independen memilih teknologi penyimpanan data microservice berdasarkan pola akses data dan persyaratan lainnya. Jika layanan mikro Anda memiliki teknologi penyimpanan data yang sama, mereka dapat menghadapi tantangan implementasi atau mengalami kinerja yang buruk. Layanan mikro lebih mudah diimplementasikan dan mencapai kinerja dan skalabilitas yang lebih baik jika mereka menggunakan penyimpanan data yang paling sesuai dengan kebutuhan mereka. Untuk informasi selengkapnya, lihat Mengaktifkan persistensi data di layanan mikro.

penilaian portofolio

Proses menemukan, menganalisis, dan memprioritaskan portofolio aplikasi untuk merencanakan migrasi. Untuk informasi selengkapnya, lihat Mengevaluasi kesiapan migrasi.

predikat

Kondisi kueri yang mengembalikan `true` atau`false`, biasanya terletak di `WHERE` klausa.

predikat pushdown

Teknik optimasi kueri database yang menyaring data dalam kueri sebelum transfer. Ini mengurangi jumlah data yang harus diambil dan diproses dari database relasional, dan meningkatkan kinerja kueri.

kontrol preventif

Kontrol keamanan yang dirancang untuk mencegah suatu peristiwa terjadi. Kontrol ini adalah garis pertahanan pertama untuk membantu mencegah akses tidak sah atau perubahan yang tidak diinginkan ke jaringan Anda. Untuk informasi selengkapnya, lihat Kontrol pencegahan dalam Menerapkan kontrol keamanan pada. AWS

principal

Sebuah entitas dalam AWS yang dapat melakukan tindakan dan mengakses sumber daya. Entitas ini biasanya merupakan pengguna root untukAkun AWS, peran IAM, atau pengguna. Untuk informasi selengkapnya, lihat Prinsip dalam istilah dan konsep Peran dalam dokumentasi IAM.

Privasi oleh Desain

Pendekatan dalam rekayasa sistem yang memperhitungkan privasi di seluruh proses rekayasa.

zona yang dihosting pribadi

Container yang menyimpan informasi tentang bagaimana Anda ingin Amazon Route 53 merespons kueri DNS untuk domain dan subdomainnya dalam satu atau beberapa VPC. Untuk informasi selengkapnya, lihat Bekerja dengan zona yang dihosting pribadi di dokumentasi Route 53.

kontrol proaktif

Kontrol keamanan yang dirancang untuk mencegah penyebaran sumber daya yang tidak sesuai. Kontrol ini memindai sumber daya sebelum disediakan. Jika sumber daya tidak sesuai dengan kontrol, maka itu tidak disediakan. Untuk informasi selengkapnya, lihat panduan referensi Kontrol dalam AWS Control Tower dokumentasi dan lihat Kontrol proaktif dalam Menerapkan kontrol keamanan pada AWS.

lingkungan produksi

Lihat lingkungan.

pseudonimisasi

Proses penggantian pengenal pribadi dalam kumpulan data dengan nilai placeholder. Pseudonimisasi dapat membantu melindungi privasi pribadi. Data pseudonim masih dianggap sebagai data pribadi.

Q

rencana kueri

Serangkaian langkah, seperti instruksi, yang digunakan untuk mengakses data dalam sistem database relasional SQL.

regresi rencana kueri

Ketika pengoptimal layanan database memilih rencana yang kurang optimal daripada sebelum perubahan yang diberikan ke lingkungan database. Hal ini dapat disebabkan oleh perubahan statistik, kendala, pengaturan lingkungan, pengikatan parameter kueri, dan pembaruan ke mesin database.

R

Matriks RACI

Lihat bertanggung jawab, akuntabel, dikonsultasikan, diinformasikan (RACI).

ransomware

Perangkat lunak berbahaya yang dirancang untuk memblokir akses ke sistem komputer atau data sampai pembayaran dilakukan.

Matriks RASCI

Lihat bertanggung jawab, akuntabel, dikonsultasikan, diinformasikan (RACI).

RCAC

Lihat kontrol akses baris dan kolom.

replika baca

Salinan database yang digunakan untuk tujuan read-only. Anda dapat merutekan kueri ke replika baca untuk mengurangi beban pada database utama Anda.

arsitek ulang

Lihat 7 Rs.

tujuan titik pemulihan (RPO)

Jumlah waktu maksimum yang dapat diterima sejak titik pemulihan data terakhir. Ini menentukan apa yang dianggap sebagai hilangnya data yang dapat diterima antara titik pemulihan terakhir dan gangguan layanan.

tujuan waktu pemulihan (RTO)

Penundaan maksimum yang dapat diterima antara gangguan layanan dan pemulihan layanan.

refactor

Lihat 7 Rs.

Wilayah

Kumpulan AWS sumber daya di wilayah geografis. Masing-masing Wilayah AWS terisolasi dan independen dari yang lain untuk memberikan toleransi kesalahan, stabilitas, dan ketahanan. Untuk informasi selengkapnya, lihat Mengelola Wilayah AWS di Referensi Umum AWS.

regresi

Teknik ML yang memprediksi nilai numerik. Misalnya, untuk memecahkan masalah “Berapa harga rumah ini akan dijual?” Model ML dapat menggunakan model regresi linier untuk memprediksi harga jual rumah berdasarkan fakta yang diketahui tentang rumah (misalnya, luas persegi).

rehost

Lihat 7 Rs.

melepaskan

Dalam proses penyebaran, tindakan mempromosikan perubahan pada lingkungan produksi.

memindahkan

Lihat 7 Rs.

memplatform ulang

Lihat 7 Rs.

pembelian kembali

Lihat 7 Rs.

kebijakan berbasis sumber daya

Kebijakan yang dilampirkan ke sumber daya, seperti bucket Amazon S3, titik akhir, atau kunci enkripsi. Jenis kebijakan ini menentukan prinsipal mana yang diizinkan mengakses, tindakan yang didukung, dan kondisi lain yang harus dipenuhi.

matriks yang bertanggung jawab, akuntabel, dikonsultasikan, diinformasikan (RACI)

Matriks yang mendefinisikan peran dan tanggung jawab untuk semua pihak yang terlibat dalam kegiatan migrasi dan operasi cloud. Nama matriks berasal dari jenis tanggung jawab yang didefinisikan dalam matriks: bertanggung jawab (R), akuntabel (A), dikonsultasikan (C), dan diinformasikan (I). Tipe dukungan (S) adalah opsional. Jika Anda menyertakan dukungan, matriks disebut matriks RASCI, dan jika Anda mengecualikannya, itu disebut matriks RACI.

kontrol responsif

Kontrol keamanan yang dirancang untuk mendorong remediasi efek samping atau penyimpangan dari garis dasar keamanan Anda. Untuk informasi selengkapnya, lihat Kontrol responsif dalam Menerapkan kontrol keamanan pada AWS.

melestarikan

Lihat 7 Rs.

pensiun

Lihat 7 Rs.

rotasi

Proses memperbarui rahasia secara berkala untuk membuatnya lebih sulit bagi penyerang untuk mengakses kredensil.

kontrol akses baris dan kolom (RCAC)

Penggunaan ekspresi SQL dasar dan fleksibel yang telah menetapkan aturan akses. RCAC terdiri dari izin baris dan topeng kolom.

RPO

Lihat tujuan titik pemulihan.

RTO

Lihat tujuan waktu pemulihan.

buku runbook

Satu set prosedur manual atau otomatis yang diperlukan untuk melakukan tugas tertentu. Ini biasanya dibangun untuk merampingkan operasi berulang atau prosedur dengan tingkat kesalahan yang tinggi.

D

SAML 2.0

Standar terbuka yang digunakan oleh banyak penyedia identitas (IdPs). Fitur ini memungkinkan sistem masuk tunggal gabungan (SSO), sehingga pengguna dapat masuk ke AWS Management Console atau memanggil operasi AWS API tanpa Anda harus membuat pengguna di IAM untuk semua orang di organisasi Anda. Untuk informasi lebih lanjut tentang federasi berbasis SAMP 2.0, lihat Tentang federasi berbasis SAMP 2.0 dalam dokumentasi IAM.

SCP

Lihat kebijakan kontrol layanan.

Rahasia

DalamAWS Secrets Manager, informasi rahasia atau terbatas, seperti kata sandi atau kredensil pengguna, yang Anda simpan dalam bentuk terenkripsi. Ini terdiri dari nilai rahasia dan metadata-nya. Nilai rahasia dapat berupa biner, string tunggal, atau beberapa string. Untuk informasi selengkapnya, lihat Rahasia dalam dokumentasi Secrets Manager.

kontrol keamanan

Pagar pembatas teknis atau administratif yang mencegah, mendeteksi, atau mengurangi kemampuan pelaku ancaman untuk mengeksploitasi kerentanan keamanan. Ada empat jenis kontrol keamanan utama: preventif, detektif, responsif, dan proaktif.

pengerasan keamanan

Proses mengurangi permukaan serangan untuk membuatnya lebih tahan terhadap serangan. Ini dapat mencakup tindakan seperti menghapus sumber daya yang tidak lagi diperlukan, menerapkan praktik keamanan terbaik untuk memberikan hak istimewa paling sedikit, atau menonaktifkan fitur yang tidak perlu dalam file konfigurasi.

sistem informasi keamanan dan manajemen acara (SIEM)

Alat dan layanan yang menggabungkan sistem manajemen informasi keamanan (SIM) dan manajemen acara keamanan (SEM). Sistem SIEM mengumpulkan, memantau, dan menganalisis data dari server, jaringan, perangkat, dan sumber lain untuk mendeteksi ancaman dan pelanggaran keamanan, dan untuk menghasilkan peringatan.

otomatisasi respons keamanan

Tindakan yang telah ditentukan dan diprogram yang dirancang untuk secara otomatis merespons atau memulihkan peristiwa keamanan. Otomatisasi ini berfungsi sebagai kontrol keamanan detektif atau responsif yang membantu Anda menerapkan praktik terbaik AWS keamanan. Contoh tindakan respons otomatis termasuk memodifikasi grup keamanan VPC, menambal instans Amazon EC2, atau memutar kredensil.

enkripsi sisi server

Enkripsi data di tujuannya, oleh Layanan AWS yang menerimanya.

kebijakan kontrol layanan (SCP)

Kebijakan yang menyediakan kontrol terpusat atas izin untuk semua akun di organisasi. AWS Organizations SCP menentukan pagar pembatas atau menetapkan batasan pada tindakan yang dapat didelegasikan oleh administrator kepada pengguna atau peran. Anda dapat menggunakan SCP sebagai daftar izin atau daftar penolakan, untuk menentukan layanan atau tindakan mana yang diizinkan atau dilarang. Untuk informasi selengkapnya, lihat Kebijakan kontrol layanan dalam AWS Organizations dokumentasi.

titik akhir layanan

URL titik masuk untuk fileLayanan AWS. Anda dapat menggunakan endpoint untuk terhubung secara terprogram ke layanan target. Untuk informasi selengkapnya, lihat Layanan AWStitik akhir di Referensi Umum AWS.

perjanjian tingkat layanan (SLA)

Perjanjian yang menjelaskan apa yang dijanjikan tim TI untuk diberikan kepada pelanggan mereka, seperti uptime dan kinerja layanan.

indikator tingkat layanan (SLI)

Pengukuran aspek kinerja layanan, seperti tingkat kesalahan, ketersediaan, atau throughputnya.

tujuan tingkat layanan (SLO)

Metrik target yang mewakili kesehatan layanan, yang diukur dengan indikator tingkat layanan.

model tanggung jawab bersama

Model yang menjelaskan tanggung jawab yang Anda bagikan AWS untuk keamanan dan kepatuhan cloud. AWSbertanggung jawab atas keamanan cloud, sedangkan Anda bertanggung jawab atas keamanan di cloud. Untuk informasi selengkapnya, lihat Model tanggung jawab bersama.

SIEM

Lihat informasi keamanan dan sistem manajemen acara.

titik kegagalan tunggal (SPOF)

Kegagalan dalam satu komponen penting dari aplikasi yang dapat mengganggu sistem.

SLA

Lihat perjanjian tingkat layanan.

SLI

Lihat indikator tingkat layanan.

SLO

Lihat tujuan tingkat layanan.

split-and-seed model

Pola untuk menskalakan dan mempercepat proyek modernisasi. Ketika fitur baru dan rilis produk didefinisikan, tim inti berpisah untuk membuat tim produk baru. Ini membantu meningkatkan kemampuan dan layanan organisasi Anda, meningkatkan produktivitas pengembang, dan mendukung inovasi yang cepat. Untuk informasi lebih lanjut, lihat Pendekatan bertahap untuk memodernisasi aplikasi di. AWS Cloud

SPOF

Lihat satu titik kegagalan.

skema bintang

Struktur organisasi database yang menggunakan satu tabel fakta besar untuk menyimpan data transaksional atau terukur dan menggunakan satu atau lebih tabel dimensi yang lebih kecil untuk menyimpan atribut data. Struktur ini dirancang untuk digunakan dalam gudang data atau untuk tujuan intelijen bisnis.

pola ara pencekik

Pendekatan untuk memodernisasi sistem monolitik dengan menulis ulang secara bertahap dan mengganti fungsionalitas sistem sampai sistem warisan dapat dinonaktifkan. Pola ini menggunakan analogi pohon ara yang tumbuh menjadi pohon yang sudah mapan dan akhirnya mengatasi dan menggantikan inangnya. Pola ini diperkenalkan oleh Martin Fowler sebagai cara untuk mengelola risiko saat menulis ulang sistem monolitik. Untuk contoh cara menerapkan pola ini, lihat Memodernisasi layanan web Microsoft ASP.NET (ASMX) lama secara bertahap menggunakan container dan Amazon API Gateway.

subnet

Rentang alamat IP dalam VPC Anda. Subnet harus berada di Availability Zone tunggal.

enkripsi simetris

Algoritma enkripsi yang menggunakan kunci yang sama untuk mengenkripsi dan mendekripsi data.

pengujian sintetis

Menguji sistem dengan cara yang mensimulasikan interaksi pengguna untuk mendeteksi potensi masalah atau untuk memantau kinerja. Anda dapat menggunakan Amazon CloudWatch Synthetics untuk membuat tes ini.

T

tag

Pasangan nilai kunci yang bertindak sebagai metadata untuk mengatur sumber daya Anda. AWS Tanda dapat membantu Anda mengelola, mengidentifikasi, mengatur, dan memfilter sumber daya. Untuk informasi selengkapnya, lihat Menandai AWS sumber daya Anda.

variabel target

Nilai yang Anda coba prediksi dalam ML yang diawasi. Ini juga disebut sebagai variabel hasil. Misalnya, dalam pengaturan manufaktur, variabel target bisa menjadi cacat produk.

daftar tugas

Alat yang digunakan untuk melacak kemajuan melalui runbook. Daftar tugas berisi ikhtisar runbook dan daftar tugas umum yang harus diselesaikan. Untuk setiap tugas umum, itu termasuk perkiraan jumlah waktu yang dibutuhkan, pemilik, dan kemajuan.

lingkungan uji

Lihat lingkungan.

pelatihan

Untuk menyediakan data bagi model ML Anda untuk dipelajari. Data pelatihan harus berisi jawaban yang benar. Algoritma pembelajaran menemukan pola dalam data pelatihan yang memetakan atribut data input ke target (jawaban yang ingin Anda prediksi). Ini menghasilkan model ML yang menangkap pola-pola ini. Anda kemudian dapat menggunakan model ML untuk membuat prediksi pada data baru yang Anda tidak tahu targetnya.

gerbang transit

Hub transit jaringan yang dapat Anda gunakan untuk menghubungkan VPC dan jaringan lokal Anda. Untuk informasi selengkapnya, lihat Apa itu gateway transit dalam AWS Transit Gateway dokumentasi.

alur kerja berbasis batang

Pendekatan di mana pengembang membangun dan menguji fitur secara lokal di cabang fitur dan kemudian menggabungkan perubahan tersebut ke cabang utama. Cabang utama kemudian dibangun untuk pengembangan, praproduksi, dan lingkungan produksi, secara berurutan.

akses tepercaya

Memberikan izin ke layanan yang Anda tentukan untuk melakukan tugas di organisasi Anda di dalam AWS Organizations dan di akunnya atas nama Anda. Layanan tepercaya menciptakan peran terkait layanan di setiap akun, ketika peran itu diperlukan, untuk melakukan tugas manajemen untuk Anda. Untuk informasi selengkapnya, lihat Menggunakan AWS Organizations dengan AWS layanan lain dalam AWS Organizations dokumentasi.

penyetelan

Untuk mengubah aspek proses pelatihan Anda untuk meningkatkan akurasi model ML. Misalnya, Anda dapat melatih model ML dengan membuat set pelabelan, menambahkan label, dan kemudian mengulangi langkah-langkah ini beberapa kali di bawah pengaturan yang berbeda untuk mengoptimalkan model.

tim dua pizza

Sebuah DevOps tim kecil yang bisa Anda beri makan dengan dua pizza. Ukuran tim dua pizza memastikan peluang terbaik untuk berkolaborasi dalam pengembangan perangkat lunak.

U

waswas

Sebuah konsep yang mengacu pada informasi yang tidak tepat, tidak lengkap, atau tidak diketahui yang dapat merusak keandalan model ML prediktif. Ada dua jenis ketidakpastian: ketidakpastian epistemik disebabkan oleh data yang terbatas dan tidak lengkap, sedangkan ketidakpastian aleatorik disebabkan oleh kebisingan dan keacakan yang melekat dalam data. Untuk informasi lebih lanjut, lihat panduan Mengukur ketidakpastian dalam sistem pembelajaran mendalam.

tugas yang tidak terdiferensiasi

Juga dikenal sebagai angkat berat, pekerjaan yang diperlukan untuk membuat dan mengoperasikan aplikasi tetapi itu tidak memberikan nilai langsung kepada pengguna akhir atau memberikan keunggulan kompetitif. Contoh tugas yang tidak terdiferensiasi termasuk pengadaan, pemeliharaan, dan perencanaan kapasitas.

lingkungan atas

Lihat lingkungan.

V

menyedot debu

Operasi pemeliharaan database yang melibatkan pembersihan setelah pembaruan tambahan untuk merebut kembali penyimpanan dan meningkatkan kinerja.

kendali versi

Proses dan alat yang melacak perubahan, seperti perubahan kode sumber dalam repositori.

Peering VPC

Koneksi antara dua VPC yang memungkinkan Anda merutekan lalu lintas dengan menggunakan alamat IP pribadi. Untuk informasi selengkapnya, lihat Apa itu peering VPC di dokumentasi VPC Amazon.

kerentanan

Kelemahan perangkat lunak atau perangkat keras yang membahayakan keamanan sistem.

W

cache hangat

Cache buffer yang berisi data saat ini dan relevan yang sering diakses. Instance database dapat membaca dari cache buffer, yang lebih cepat daripada membaca dari memori utama atau disk.

data hangat

Data yang jarang diakses. Saat menanyakan jenis data ini, kueri yang cukup lambat biasanya dapat diterima.

fungsi jendela

Fungsi SQL yang melakukan perhitungan pada sekelompok baris yang berhubungan dengan catatan saat ini. Fungsi jendela berguna untuk memproses tugas, seperti menghitung rata-rata bergerak atau mengakses nilai baris berdasarkan posisi relatif dari baris saat ini.

beban kerja

Kumpulan sumber daya dan kode yang memberikan nilai bisnis, seperti aplikasi yang dihadapi pelanggan atau proses backend.

aliran kerja

Grup fungsional dalam proyek migrasi yang bertanggung jawab atas serangkaian tugas tertentu. Setiap alur kerja independen tetapi mendukung alur kerja lain dalam proyek. Misalnya, alur kerja portofolio bertanggung jawab untuk memprioritaskan aplikasi, perencanaan gelombang, dan mengumpulkan metadata migrasi. Alur kerja portofolio mengirimkan aset ini ke alur kerja migrasi, yang kemudian memigrasikan server dan aplikasi.

CACING

Lihat menulis sekali, baca banyak.

WQF

Lihat Kerangka Kualifikasi Beban Kerja AWS.

tulis sekali, baca banyak (WORM)

Model penyimpanan yang menulis data satu kali dan mencegah data dihapus atau dimodifikasi. Pengguna yang berwenang dapat membaca data sebanyak yang diperlukan, tetapi mereka tidak dapat mengubahnya. Infrastruktur penyimpanan data ini dianggap tidak dapat diubah.

Z

eksploitasi zero-day

Serangan, biasanya malware, yang memanfaatkan kerentanan zero-day.

kerentanan zero-day

Cacat atau kerentanan yang tak tanggung-tanggung dalam sistem produksi. Aktor ancaman dapat menggunakan jenis kerentanan ini untuk menyerang sistem. Pengembang sering menyadari kerentanan sebagai akibat dari serangan tersebut.

aplikasi zombie

Aplikasi yang memiliki CPU rata-rata dan penggunaan memori di bawah 5 persen. Dalam proyek migrasi, adalah umum untuk menghentikan aplikasi ini.

Terjemahan disediakan oleh mesin penerjemah. Jika konten terjemahan yang diberikan bertentangan dengan versi bahasa Inggris aslinya, utamakan versi bahasa Inggris.